NCI Agency
Costed Customer Services Catalogue v9.0

2025 Service Rates

Annex A to NCIA/COO/2024/01003

NATO
OTAN

NATO Communications
and Information Agency

This page is left blank intentionally

2025 Service Rates v9.0

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
WORKPLACE SERVICES				
WPS001	Managed Device Service	WPS001	Per Device	886
		WPS001-1 Portable (Laptop / Tablet) including obsolescence refresh	Per Device	1,477
WPS002	Enterprise Identity Access Management Service (Former User Access Service)	WPS002-1 User Account	Per User Account	98
		WPS002-2A Web Federation*	Per Connection	4,695
		WPS002-2B DNS Federation*	Per Connection	511
		WPS002-3: Data Directory Synchronization	Per Connection	3,431
WPS003	Enterprise User LicenseService	WPS003-1 Standard User	Per User	581
		WPS003-2 Light User	Per User	Retired. All former Light Users become Standard User
		WPS003-3 NATO Delegation User*[1]	Per Device	434
WPS006	REACH Mobile Workplace Service		Per Device	2,272
WPS007	Print/ Scan/Copy Service	WPS007-1-A: A3 Large Print Volume MFD	Per Device	2,090
		WPS007-1-B: A3 MFD	Per Device	1,440
		WPS007-1-C A4 MFD	Per Device	1,240
		WPS007-1-D: A4 Desktop-sized MFD	Per Device	890
		WPS007-2: NONO	Per Device	849

[1] Up to 8 users per device.

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
		Device		
		Black & White paper	Per Page	0.0077
		Colour paper	Per Page	0.0238
		Stapler finisher	1	250
		Booklet finisher	1	475
		High volume document feeder	1	100
		Hole puncher	1	75
WPS008	Enterprise Services Operations Centre Service		Per Device	Included in the Service Rate of WPS001, WPS006, WPS016-A
WPS009	Unclassified Voice Collaboration Service	WPS009-1: Voice Collaboration (Calling) Service	Per Telephone Number[2]	245
		WPS009-2: Business-to-Business Federation (B2B)	Per instance	9,028
WPS010	Video (VTC) Collaboration Service	WPS010-1: Soft Client*	Per Client Device	301
		WPS010-2: VTC System Only		15,830
		WPS010-3: Desktop Dedicated Terminal		5,127
		WPS010-4: VTC Room - Roll About SDS*		17,305
		WPS010-5: VTC Room - Roll About DDS		23,343
		WPS010-6: VTC Room - 15 person		26,315
		WPS010-7: VTC Room - 25 person		28,562

[2] For 2023 quantities customers will use previous unit of measure (device). The NCI Agency will do the mapping to the new unit of measure (telephone numbers).

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
		WPS010-8: VTC Room - 50 person		35,649
		WPS010-9: VTC Room - 175 person		43,480
		WPS010-10: Immersive Telepresence Meeting(ITP) Room		44,488
		WPS010-11: B2B connection	Per B2B Package	23,940
WPS012	Workstream Collaboration Service	Workstream Collaboration Service[3]	Per user	51
WPS014	Secure Voice Service	WPS014-1: Secure Voice Service	Per Device	492
		WPS014-2: Secure Mobile Phone		3,837
		WPS014-4: Business-to-Business Federation (B2B)		12,117
WPS015	Voice Loop Service[5]			
WPS016	Enterprise Managed Mobility Service (WPS008 is mandatory with flavour WPS106-A)	WPS016-A: Smartphone/Tablet (iOS only)	Per device	502
		WPS016-B1: Cellular Subscription (Profile Plan 1 - Basic)	Per SIM card	200
		WPS016-B2: Cellular Subscription (Profile Plan 2 - Standard)	Per SIM card	300
		WPS016-B3: Cellular Subscription (Profile Plan 3 -	Per SIM card	360

[3] Rate applies to new quantities (2023 onwards).

[5] To be determined under AMDC2 POW.

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
		Traveller)		
		WPS016-B4: Cellular Subscription (Profile Plan 4 - Traveller Unlimited)	Per SIM card	450
		WPS016-B5: Cellular Subscription (Profile Plan 5 - Data Plan Hotspot)	Per SIM card	360
		WPS016-C: Enterprise Managed Mobility Service (NU/NR)	Per Device	266
		WPS016-5: Multi-Factor Authentication Token (OTP) [6]	Per Device	32
		Mobile Secure Communication on smartphones - SecuSUITE	Per Connector	433
INFRASTRUCTURE SERVICES				
INF001	Local Area Network (LAN) Service		Per Port	147
INF002	NATO General Purpose Communication System (NGCS) Point of Presence (POP) Service	AirC2IS POP[9]	Per PoP	
		INF002P - Pico POP	Per PoP	51,861
		INF002L - Legacy PoP* (incl. NNCCRS non-collocated)	Per PoP	21,669
		INF002NNG - NATO-Nations Gateway Option	Per Gateway	4,386
		INF002LVAR - Local V2 Aggregation	Per Router	5,943

[6] Rate applies to existing quantities of tokens (2022 SLAs), flavour no longer available for new requests.

[9] To be determined under AMDC2 POW.

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
		Router		
		INF002NCI - NCI Point of Presence	Per PoP	123,774
		INF002NLI - NGCS Legacy Infrastructure	1	1,319,200
INF003	Enterprise Internet Access Service		1	6,265,263
INF004	INF004 Infrastructure Virtualization Service		Per Infrastructure Unit	5,349
	INF004-2 SMC Discovery and Truesight		1	422,000
	INF004-3 Packaging		1	452,423
INF005	Infrastructure Integration Service		1	Under INF004 Pricing
INF006	NATO Enterprise Directory Service (NEDS)		1	1,376,689
INF007	Infrastructure Storage Service		1	Under INF004 Pricing
INF012	SATCOM Service		1	27,540,488
INF013	Very Low Frequency (VLF) Broadcast Service		1	5,014,965
INF014	Transmission Service		1	13,929,263
INF015	Broadcast, Maritime Rear Link and Ship-Shore (BRASS) STIV RMD		1	627,724
INF016	Infrastructure Backup Service		1	Under INF004 Pricing
		INF020-1 Laptop	Per Device	150

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
INF020	Deployable CIS EquipmentPool (DCEP) Service	INF020-2 Desktop	Per Device	149
		INF020-3 Monitor	Per Device	47
		INF020-4 Printer/MFD	Per Device	149
		INF020-5 Scanner	Per Device	75
		INF020-6 Phone	Per Device	41
		INF020-7 VTC Kit	Per Device	863
		INF020-8 Projector	Per Device	51
		INF020-9 Switch	Per Device	519
		INF020-10 Fiber reel	Per Device	160
		INF020-11 KVM Switch	Per Device	41
		INF020-12 Core GIS Kit Types 2 & 3	Per Device	4,567
		INF020-13 Core GIS Kit Type 1	Per Device	8,510
		DF BoB	Per Device	156
		Media Convertor	Per Device	29
		Webcam	Per Device	26
INF023*	Network Services Fulfilment(NSF) Service	Establishment/Modific ation	Per Connection	3,278
		Activation/Deactivation	Per Connection	927
INF028	ACCS Sensor IntegrationModule (ASIM) Service[11]			

[11] To be determined under AMDC2 POW

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
INF034	Recognized Air Picture (RAP) Dissemination Service[12]			
INF035	DCIS – Deployable Nodes Service	DragonFly (INF008)	Per System	533,891
		Limited Interim NATO Response Force (NRF) CIS-Expansion (LINC-E) (INF009)	Per System	302,956
		Communications Gateway Shelters (CGS) (INF010)	Per System	552,190
		In-Theatre Mobile CIS Detachment (IMCD) (INF017)	Per System	273,752
		Mini Point of Presence (Mini-PoP) (INF018)	Per System	63,755
		Theatre Liaison Kit (TLK/ILK) (INF019)	Per System	35,288
		Theatre Liaison Kit (TLK/ILK) STK (INF019-1)	Per System	36,230
		Afloat Command Platform (ACP) (PLT007)	Per System	267,505
		DCIS – Remote Network Module (RNM) (INF045)	Per System	47,832
		Maritime Command and Control Platform (MAR C2P) Single Domain (PLT012-1)	Per System	141,141

[12] To be determined under AMDC2 POW

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
		Maritime Command and Control Platform (MAR C2P) Dual Domain (PLT012-2)	Per System	197,962
		SEMARCIS/SEMARCOM Deployable Maritime CIS (INF044)	Per System	47,040
		Signal Support Group(SSG) (SEC021)	Per System	93,851
INF036	DCIS – Deployable SATCOMService	TSGT (INF021)	Per System	125,982
		DSGT (INF022)	Per System	51,253
		DART/Fast Small (INF032)	Per System	31,813
INF037	DCIS – Deployable RadioTransmission Service	HF (INF024-1) – HF Shelter	Per System	31,732
		HF (INF024-2) – HF T-Case	Per System	17,485
		DLOS (INF025)	Per System	17,890
INF038	DCIS – Deployable NodesAnchor Service	Mission Preparation Centre Service (INF027)	Per System	26,454
		DOG (INF026)	Per System	706,988
INF040	UHF TACSAT Radio Services	INF040-1: On The Pause (OTP), Portable back-pack configuration	Per Radio	2,668
		INF040-1: On The Move (OTM), Vehicle- or mobile-mounted configuration	Per Radio	2,668
		INF040-1: Static Radio Site	Per Radio	2,668

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
		INF040-2: TACSAT Site infrastructure support service	Per Site	24,068
INF041	CRC System Interface Service (CSI) Local SupportService		Per Deployment	32,319
INF043	NATO Partner Network		1	424,191
INF046*	NRA – IPv6 Local Internet Registry (LIR)	INF046-D IPv6 Sponsoring LIR NRA	Per Allocation	4,232
INF048	Data Science Infrastructure as a Service		Per IaaS Unit	22,852
		Advanced IaaS	Per User	3,600
INF053	Internet Website Publishing and Protection Service	INF053-1 Standard	Site (URL)	17,512
PLATFORM SERVICES				
PLT001	Information Sharing and Collaboration Platform Services	PLT001-4: NATO Enterprise Collaboration Platform - Basic Plan	Per Portal URL	4,063
		PLT001-5: NATO Enterprise Collaboration Platform – Advanced Plan	Per Portal URL	15,691
		PLT001-6: COI Portal Service - Basic Plan	Per Portal URL	4,064
		PLT001-7: COI Portal Service - Advanced Plan	Per Portal URL	10,825

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
PLT002	CFBLNet	PLT002-1: CFBLNet for NATO organisations only - Base	Per Organization	72,284
		PLT002-2: CFBLNet services for NATO organisations only (Extra NKIT)		9,346
PLT003	Web Hosting Service	PLT003-1: Dedicated Standalone	Per GB	53
		PLT003-2: Dedicated with DR	Per GB	72
		PLT003-3: Dedicated with HA	Per GB	88
		PLT003-4: Dedicated with HA and DR	Per GB	118
		PLT003-5: Shared Platform on-Prem	Per GB	44
		PLT003-6-A: Shared Platform Cloud – 10GB	Per GB	1,080
		PLT003-6-B: Shared Platform Cloud Beyond 10GB +	Per GB	595
PLT004	Service Oriented Architecture & IdentityManagement		1	3,529,587
PLT006	Database Platform Service	PLT006-1 Shared Database Platform	GB	36
		PLT006-2A Dedicated Standalone	GB	37
		PLT006-2B Dedicated with High Availability	GB	45
		PLT006-2C Dedicated with Disaster Recovery	GB	42

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
		PLT006-2D Dedicated with High Availability and Disaster Recovery	GB	50
		PLT006-3 Oracle Technology Product Licenses	1	1,536,577
PLT008	DevSecOps Service	NSF Standard Profile:	User/Month	83
		NSF JIRA Profile	User/Month	54
		NSF ADO Profile:	User/Month	34
		NSF GitLab Profile	User/Month	34
		NSF Power BI Profile	User/Month	19
		NSF Stakeholder Profile	10 Users/Year	1,440
		NSF Stakeholder Profile	50 Users/Year	6,000
		NSF Stakeholder Profile	100 Users/Year	9,600
		NSF Private Cloud – Small	Project/Year	15,000
		NSF Private Cloud – Medium	Project/Year	22,500
		NSF Private Cloud – Large	Project/Year	30,000
		Non-common-funded Customer – Options:		
		Azure DevOps	User/Month	5
		Azure Credits	Unit/Month	84
		Jira	User/Month	20
		SonarQube	100,000 lines of code/Year	480

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
		DevSecOps – SME Support	Hour	130
		Managed Endpoint	Device/Month	42
		NEXUS IQ + Firewall	User/Month	58
		NATO Trusted Container Registry – small	Project/Year	5,000
		NATO Trusted Container Registry – medium	Project/Year	13,000
		NATO Trusted Container Registry – large	Project/Year	20,000
PLT009	Electronic Definitive Media Library (EDML) Service	Multi-tenant Media Delivery (SaaS)	Per Instance	38,318
PLT010	Cloud Services Management and Integration Service - Office 365	PLT010-1A MarIE Start pack (up to 50users)	1	75,310
		PLT010-1B MarIE Additional users (> 50)	Per User	625
		PLT010-2A Resource Consumption Start pack (min 4 credit)	1	7,200
		PLT010-2B Resource Consumption – Additional Credit	Per Credit	1,800
PLT011	Cloud Applications Access (CloudApp) Service		Per CCU	279
PLT013	NATO Integrated Secure Platform Service (NISP)[13]			

[13] To be determined under AMDC2 POW

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
PLT018	Data Science Platform as a Service	PLT018-1 Data Science Profile	Per Profile (annual)	25,407
		PLT018-2 Advanced Analytics Profile	Per Profile (annual)	16,304
		PLT018-3 Machine Learning Profile	Per Profile (annual)	16,304
		PLT018-4 Big Data Profile	Per Profile (annual)	16,304
		Advanced (PaaS) User Profile [14]	Per User (annual)	3,600
SUBJECT MATTER EXPERTISE SERVICES				
SME001	Chief Quality Office Subject Matter Expertise Service		1	170,584
SME002	Independent Verification and Validation for A2SL Service		1	2,008,171
SME004	Provision of Subject Matter Expertise for the Federated Mission Networking (FMN Framework)		1	1,966,766
SME005	Acquisition Services		1	Not Separately priced
SME007*	Operational Application Support Service	SME007-1: Regular FAS OPS – Bundle B	Per Site	21,897
		SME007-2: Regular FAS OPS – Bundle C	Per Site	19,530
		SME007-3: Regular FAS OPS – Bundle D	Per Site	19,530
		SME007-4: Regular FAS OPS – Bundle E	Per Site	17,253

[14] Advanced (PaaS) User Profile is a prerequisite to all profiles.

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
		SME007-5: Regular FAS OPS – On-Site Support Option	Per Site/Per Bundle	2,875
		Regular FAS OPS – Complete	Per Site	92,585
SME008	Maritime Operational CIS Deployment and Recovery Service	SME008-1: Collocated Major Handover	Per Handover	38,531
		SME008-2: Non-Collocated Major Handover	Per Handover	58,637
		SME008-3: NATO Control and Reporting Centre (CRC) System Interface (CSI) Deployment / Recovery (DR)	Per deployment	22,168
		SME008-4: SEMARCIS / SEMARCOM Deployment / Recovery (DR	Per deployment	12,207
		SME008-5: Tactical Satellite (TACSAT) Deployment / Recovery (DR)	Per deployment	14,347
SME009	Subject Matter Expertise Services to support the NCSas an Affiliate to the Federated Mission Networking (FMN)			1,836,215
SME010	ACP127 Message OperatorService		Per Signal Message Address (SMA)	728

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
SME012	VeVA CIAVSupport		1	2,408,497
SME014	Provision of Subject Matter Expertise to Support the Governance and Management of the VeVA Mission Network[15]		1	
SME022	Maritime Broadcast Operations Service[16]		1	480,015
APPLICATION SERVICES				
APP002	Shared Early Warning (SEW)Application Service	APP002	1	476,262
		APP002F* Federated	Connection	13,431
APP005	CBRN Application Service		1	503,838
APP006	Ballistic Missile Defence (BMD) System of SystemsManagement Service[17]			
APP007	TOPFAS Application Service		1	4,027,362
APP009	INT-Core Application Service	APP009-1 Large Site	Per site / domain	430,692
		APP009-2 Medium Site	Per site / domain	252,591
		APP009-3 Small Site	Per site / domain	120,906

[15] Due to the introduction of VeVa Mission Concept, the rate is not yet finalized as discussions are on-going with budget holders. Discussions on funding streams to be finalized by end of 2Q24.

[16] Applicable only to MARCOM SLA.

[17] To be determined under AMDC2 POW

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
APP010	NIRIS Application Service[18]			
APP011	OANT Application Service		1	301,072
APP012	SMACQ Application Service		1	300,927
APP013	DISG Application Service[19]	APP013-1 Product management	Per Site	243,042
		APP013-2AD DISG Standard connection – small - deployment	Per Site	15,529
		APP013-2A DISG Standard connection – small	Per Site	23,380
		APP013-2BD Standard connection – medium – deployment	Per Site	20,700
		APP013-2B Standard connection - medium	Per Site	46,761
		APP013-2CD DISG Standard connection – large – deployment	Per Site	24,973
		APP013-2C DISG Standard connection – large	Per Site	70,139
		APP013-2DD Diode deployment	Per Site	8,639
		APP013-2D Diode	Per Site	23,380
APP015	JCHAT Application Service[20]			
APP016	JTS/FAST Application Service[21]			

[18] To be determined under AMDC2 POW

[19] Deployment rate is applicable only once for new sites, however for SHAPE instances the rate is applied yearly.

[20] To be determined under AMDC2 POW

[21] To be determined under AMDC2 POW

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
APP017	Land C2 Application Service		1	2,009,008
APP018	MCCIS Application Service		1	1,789.194
APP019	White Shipping Application Service		1	598,290
APP021	JOCWatch Application Service	APP021 Centralised	1	799,762
		APP021F* Federated	Connection	28,877
APP022	NCOP Application Service	APP022 Centralised	1	3,496,947
		APP022F* Federated	Connection	44,877
APP023	NAMIS Application Service		1	2,132,933
APP025	Naval Mine Warfare Support Service		1	253,514
APP026	Virtual Battle Simulation (VBS) Application Service		1	17,148
APP027	NATO Nuclear C2 Reporting Application Service		1	1,048,345
APP028	NATO Nuclear Planning Application Service		1	2,358,174
APP029	Military Message Handling Application Service		1	2,820,587
APP030	Tasker and Project Tracker Applications Service (TT+and PITT)	APP030-1: TT+	Per User	149
		APP030-2: PITT	Per User	43
APP031	Enterprise Document Management Application Service (EDMS)		Per User	150

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
APP032	Personnel Management Application Service	APP032-1 APMS	Per User	43
		APP032-2 ERT	Per User	4
		APP032-3 Sequence	Per User	11
		APP032-4 AMIS Core	Per User	42
		APP032-4.1 AMIS Kiosk	Per Kiosk	674
		APP032-4.2 AMIS Web Enrolment	Per Enrolment	218
		APP032-5 NSTEP	Per User	10
		APP032-6 NIACS	Per User	7
		APP032-7 ISIPS	Per User	15
		APP032-8 HR-Portals	Per User	1
APP033	INTEL FS Application Service		1	4,980,662
APP034	Integrated Engineering Management (IEMS) Application Service		1	343,669
APP036	Finance (FinS) Application Service		1	1.929.369
APP041	Logistics Functional Area Services (LOGFAS) Application Service		1	3,844,131
APP043	Interactive Simulation Package (ISP) Application Service[22]			
APP045	SIGINT COINS Application Service		1	1,760,383
APP046	HMART Application Service		1	278,188

[22] To be determined under AMDC2 POW

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
APP047	AOSS Application Service		1	4,101,363
APP048	Analyst Notebook (ANB) Service		1	170,366
APP049	Integrated Command and Control (ICC) Application Service	NCS-wide ICC software maintenance and in service support (AIRC2 POW)[23]		
		ICC Client Site Support* ICC Client Support*	Per Site Site Rate + Client Rate x [number of clients]	2,802 98
		ICC Server support*	Per Installation	20,277
APP050	Air Command and Control Systems (ACCS) Application Service[24]			
APP052	Air Situation Data Exchange (ASDE) Gateway Service	NCS-wide ICC software maintenance and in service support (AIRC2 POW)[25]		
		ASDE Gateway Service -National Instance*	Per Instance	108,082
APP053	Multi Airborne Early Warning Ground Integration Segment (AEGIS) Site Emulator (MASE)			

[23] To be determined under AMDC2 POW

[24] To be determined under AMDC2 POW

[25] To be determined under AMDC2 POW

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
	Application Service[26]			
APP054	L16@29k Application Service[27]			
APP055	Core Geographic Information System (GIS) Application Service		1	5,909,127
APP056	ISR Collection ManagementTool (ICMT) Application Service		1	1,071,772
APP057	INTEL FS SIGINT Capability(ISC) Application Service		1	415,137
APP058	Release Server ApplicationService		1	258,570
APP059	Joint Exercise and Management (JEMM)Application Service		1	724,162
APP060	ISR Coalition Shared Data (CSD) Application Service		1	339,769
APP061	AirC2IS Application Service	NCS-wide ICC software maintenance and in service support (AIRC2POW)[28]		
		AirC2IS Client support*	Per Client	268

[26] To be determined under AMDC2 POW

[27] To be determined under AMDC2 POW

[28] To be determined under AMDC2 POW

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
		AirC2IS Server support*	Per instance (standard HA server cluster)	101,063
APP064	ITSM Toolset Application Service			Included in the Service Rate of WPS001,WPS006 , WPS016-A
APP065	Joint Tactical Simulation (JCATS) Application Service		1	94,172
APP066	Joint Operational Simulation (JTLS) Application Service Centralised Capability		1	280,001
	APP066-1 Joint Operational Simulation (JTLS) Approved Additional Modules Service		1	110,329
APP067	RECCEN Application Service		Per user	13
APP068	Advisor Network (ANET) Application Service	Small	Per Deployment	292,061
		Medium	Per Deployment	411,029
		Large	Per Deployment	563,094
APP069	Air Integrated Training Capability (ITC) Application Service[29]			
APP070	Training Objective Management Module (TOMM) Application Service		1	101,019

[29] To be determined under AMDC2 POW

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
APP074	NATO Lessons Learned Portal (NLLP) Application Service		1	143,496
APP075	EW FS Application Service		1	654,937
APP076	I&W Application Service		1	167,703
APP078	ORION Space Domain Application Service		1	447,117
APP079	NATO Automated Biometrics Identification (NABIS) Application Service		1	302,113
APP081	Joint Advanced Distributed Learning (JADL) Service		1	312,519
APP082	Digital Emergency Alert Notification Service		Per Managed Device	33
APP083	Mission Planning Application Service for Dual Capable Aircraft[30]			
APP084	ISMERLO Application Service		1	381,946
APP085	Housing Office Management Application Service		1	33,245
APP086	NATO Information Portal (NIP)		Per User	155
APP099	Data Science Software as a Service	APP099-1 Power BI Dynamics Dashboards	Per Unit (Portal)	7,007
		APP099-2 KNIME Self-Service Analytics		8,003

[30] To be determined under AMDC2 POW.

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
		APP099-3 Jupyter Laboratory		3,607
		APP099-4 GitLab Project Portal		2,574
		APP099-5 MinIO Data Portal		1,269
		APP099-6 Hosted LLM Services		1,269
		Advanced (PaaS) User Profile	Per User	3,600
		Portal (SaaS) User Profile		1,680
		Portal (SaaS) Consumer Profile		324
APP100	Mobile Advisor Reporting Tool (MART)	APP100-1 Small Deployment (0-200 Users)		58,696
		APP100-2 Medium Deployment (200-2,000 Users)		68,130
		APP100-3 Large Deployment (2,000-10,000 Users)		77,699
APP102	REACT – PNT and NAVWAR Application Service		1	87,432
APP103	Business Process Management Application Service (BPM) Service		Per User	11
APP104	Medical Management Application Service		1	316,063
APP107	NATO Unclassified Artificial Intelligence ChatBot		1	501
APP108	NATO Maritime Availability Database (NMAD)		1	263,391
SECURITY SERVICES				
SEC001	Security Accreditation Support Service		1	1,300,664

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
SEC004	Cyber Security Analysis Service		1	2,690,690
SEC005	NATO Cyber Defence Rapid Reaction Team (RRT) / Security Response Team		1	320,621
SEC006	Cyber Security Incident Management Service		1	2,777,439
SEC007	Cyber Security Monitoring Service		1	10,711,292
SEC008	Cyber Security OPCEN Helpdesk Service		1	1,689,402
SEC009	Cyber Security Outreach Service		1	652,830
SEC010	Cyber Security Information Sharing Service		1	3,882,462
SEC011	Gateway Security Service		1	4,239,620
SEC012	CIS End-point Protection Support Service		Per Endpoint	17
SEC013	Crypto Compliance Support Service		1	290,315
SEC014	Crypto Management and Logistic Support Service		1	4,672,831
SEC015	Security Certificate Service		1	2,376,943
SEC019	Cyber Operations & Exercises		1	537,368
SEC020	Cyber Security Management Service		1	3,561,901
SEC022	Sensor and Flight Plan Boundary Protection System (BPS) Application			

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
	Service[31]			
SEC023	Penetration Testing Service	SEC023-1-A: Web Application Penetration Test - small	Per Penetration Test Size	18,632
		SEC023-1-B: Web Application Penetration Test - medium	Per Penetration Test Size	36,768
		SEC023-1-C: Web Application Penetration Test - large	Per Penetration Test Size	76,668
		SEC023-1-D: Web Application Penetration Test - regression test	Per Penetration Test Size	12,586
		SEC023-1-E: Web Application Penetration Test - OWASP ASVS	Per Penetration Test Size	24,980
		SEC023-1-F: Web Application Penetration Test - WASA BlackBox	Per Penetration Test Size	22,749
		SEC023-1-G: Web Application Penetration Test - WASA Grey Box	Per Penetration Test Size	23,504
		SEC023-2-A: Network/Infrastructure Penetration Test - small	Per Penetration Test Size	24,053
		SEC023-2-B: Network/Infrastructure Penetration Test - medium	Per Penetration Test Size	42,491
		SEC023-2-C: Network/Infrastructure Penetration Test -	Per Penetration Test Size	81,787

[31] To be determined under AMDC2 POW

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
		large		
		SEC023-2-D: Network/Infrastructure Penetration Test - regression test	Per Penetration Test Size	18,309
		SEC023-3-A: Application Penetration Test - light	Per Penetration Test Size	9,211
		SEC023-3-B: Application Penetration Test - small	Per Penetration Test Size	18,582
		SEC023-3-C: Application Penetration Test - medium	Per Penetration Test Size	37,020
		SEC023-3-D: Application Penetration Test - large	Per Penetration Test Size	76,316
		SEC023-3-E: Application Penetration Test - Regression Test	Per Penetration Test Size	12,838
SEC024	Vulnerability Assessment Service	SEC024-1: Vulnerability Assessment - Extra small	Per Assessment Size	19,749
		SEC024-2: Vulnerability Assessment - Small	Per Assessment Size	36,092
		SEC024-3: Vulnerability Assessment - Medium	Per Assessment Size	70,255
		SEC024-4: Vulnerability Assessment - Large	Per Assessment Size	102,922

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
		SEC024-5: Vulnerability Assessment - Extra large	Per Assessment Size	162,039
SEC025	Emission Security Service		1	793,109
SEC026	Attack Surface Reduction Service		1	1,089,016
SEC027	Continuous Security Posture Assessment Service	SEC027-1 Online Vulnerability Assessment and Remediation Support – Small	Per Site/ Network	11,048
		SEC027-2 Online Vulnerability Assessment and Remediation Support – Medium	Per Site/ Network	27,267
		SEC027-3 Online Vulnerability Assessment and Remediation Support – Large	Per Site/ Network	42,547
		SEC027-4 Online Vulnerability Assessment and Remediation Support – XLarge	Per Site/ Network	59,663
		SEC027-5 External Attack Surface Monitoring	1	240,162
SEC028	Vulnerability Management Service		1	1,110,620
SEC029	Cyber Security Platform and Infrastructure Service		1	6,560,020
SEC030	Cyber Threat Hunting Service		1	2,074,279

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
SEC032	Adversary Emulation Service		1	1,477,885
SEC033	Cyber Security Architectural Coherency and Roadmaps Service		1	1,534,885
TRAINING SERVICES				
TRA003	Education and Individual Training Availability and Maintenance (EIT A&M)		1	3,987,983
LOGISTIC SUPPORT SERVICES				
LOG001	CIS Asset & Materiel Management		1	3,514,291
LOG002	Test Equipment Verification and Maintenance Service –3rd Level		1	840,122
LOG003	Test and Evaluation of Electromagnetic Environmental Effects Service – 3rd Level		1	464,330
LOG005	Support to Exercises with Deployable CIS Equipment Pool (DCEP) Service		1	764,902
OTHER SERVICES				
OTH001	Service Management and Control Function Service		1	Not Separately Priced
		Non-common Funded Customer	1	5% of the total cost of the SSP

Service ID	Service Name	Service Flavour /Option	Service Unit	Service Rate v9.0 In-service – support (EUR)
OTH002	Account Management Service	Service*		
		Global Enterprise (CSLA)	Per agreement	240,141
		Enterprise Agreement (eSLA)	Per agreement	109,335
		Local SLA	Per agreement	80,052
OTH003	AirC2 In Service Support Program of Work (ISS POW)General Support Service[32]			
OTH004	DCIS – Management Support Service		1	Not separately priced
OTH005	Training Capability BattleLab Support Service		1	971,866
NATO DIGITAL WORKPLACE SERVICES				
NDW005	Digital Events Service	NDW005-A Digital Event	1	4,152
		NDW005-B Digital and Hybrid Event	1	6,100

*** Service available only to External NCI Agency Customers**

[32] To be determined under AMDC2 POW

2025 Service Rates for NATO HQ only

Service ID	Service Name	Service Flavour	Service Unit	Network Classification	Initiation Cost (NATO/ NATIONS)	In-Service Support Cost NATO	In-Service support Cost NATIONS	Lifecycle Recovery Cost NATIONS	Life-time (years)
						Annual in EUR			
WPS001N	Managed Devices		End-User Device						
		Thick client							
				All	1372	784	178	274	5
		Thin client							
				All	1125	783	177	225	5
		Laptop							
				Business Network	1815	792	186	605	3
		Tablet							
				Business Network	1202	759	153	401	3
		Common Use Thin Client							
				All	584	628	51	116	5
		Options							
			Additional Monitor 21"		n.a.	12	12	27	5
			Additional Monitor 24"		260	20	20	52	5
			KVM Switch		360	7	7	75	5
			Headset		35	n.a.	n.a	n.a	n.a.
			USB Camera		103	n.a.	n.a.	n.a.	n.a
WPS002N	User Access Service								
		User Account / Password							
				All	76	81	21	n.a.	n.a.
		User Token (Smart- Card)							
				NATO Secret (ON)	160	3	3	n.a.	n.a.

WPS003	Enterprise User License Service		Physical User						
		Light User (incl. Premier Support)			Retired	Retired	Retired	n.a.	n.a.
		Standard User (incl. Premier support)			1,521	580	580	n.a.	
WPS007N	Print/Scan/Copy Service		Print Device						
		Workgroup printer/Scanner	Co-Co						
		WPS007-A	Device	All	n.a.	2.090	2.090		5
			Booklet Finisher			475	475		
			High Volume Feeder			100	100		
			Hole Puncher			75	75		
		WPS007-B	Device	All	n.a.	1.440	1.440		5
		WPS007-C	Device	All	n.a.	1,240	1.240		5
		WPS007-D	Desktop-sized Device	All	n.a.	890	890		5
		Customer Owner* Printers (Installation)							
			Stand Alone Printer	All	102	n.a.	n.a.		
			Network Printer	All	207	n.a.	n.a.		
			Multi-Function Printer (MFP)	All	552	n.a.	n.a.		
		Price per page							
			B/W		n.a.	0.0077	0.0077		
			Colour		n.a.	0.0238	0.0238		
WPS009N	Voice Collaboration Service		End-User Device						
		Soft client							
					0	208	N/A		
		Desk phone							
			Hallway Phone	Unclassified	Not separately orderable	224	13		
			Desk Phone		180	224	13		

WPS010N	Video (VTC) Collaboration Service		End-User Device						
		Soft Client							
				All	0	0	0		
		VTC Round Table							
				All	TBD	681	681		
		VTC Roll about							
				All	TBD	993	993		
		VMR-VTC Conference room							
				All		18,519	4,080		
		VMR Room							
				All	TBD	58,293	N/A		
WPS011N	IPTV Service		End-User Device						
		Soft Client							
				All	0	1324	1324		
		IPTV Client							
			Set-top box	All	524	1324	1324		
			55"IPTV setup	All	1,980	1399	1399		
			65"IPTV setup	All	3,670	1399	1399		
WPS012	Collaboration		User Account						
					51	51	51		
WPS0016 N	Enterprise Managed Mobility Services		End-User Device						
		Smartphone							
			IPhone	Unclassified	747	171	150		
INF001N	Local Area Network (LAN) Service		Port						
				All	Subject to Price Proposal	125	43		
INF003	Enterprise Internet Access		Unit 1						
					N.A.	1,612,424	N.A.		
INF004N-16N	IaaS		Unit 1						
				All	Subject to Price Proposal	2,040,000	N.A.		

This page is left blank intentionally

NCI Agency
Costed Customer Services Catalogue v9.0

2025 Service Descriptions

Enclosure to NCIA/COO/2024/01003

NATO
OTAN
NATO Communications and Information Agency

This page is left blank intentionally

NATO OTAN

NATO Communications and Information Agency

Table of Contents

NATO
OTAN
NATO Communications and Information Agency
NCI AGENCY

Introduction to the NCI Agency Costed Customer Services Catalogue

This page is left blank intentionally

Record of Changes

Due to large amount of changes in each version of the catalogue, the Record of Changes table below only lists the latest changes that are introduced in this current version.

9.0 Release record of changes

Change category	Details
New Services/Flavours	• NATO Digital Workplace Services Portfolio Grouping has been added. • The following services have been added with pipeline status: NDW001 NATO Digital Workplace Service (Low Side), NDW003 Hybrid Work Environment - Managed Device Service, NDW004 Hybrid Work Environment - Audio-Visual Services. • NDW005 Digital Events Service has been added as a new service. • SEC032 Adversary Emulation Service and SEC033 Cyber Security Architectural Coherency and Roadmaps have been added as new cyber security services. • The following Data Science services have been added: INF048 Data Science Infrastructure as a Service, PLT018 Data Science Platform as a Service, APP099 Data Science Software as a Service. • APP107 NATO Unclassified Artificial Intelligence ChatBot has been added as a new service. • APP009 INT-Core Application Service, APP100 Mobile Advisor Reporting Tool (MART), APP102 REACT – PNT and NAVWAR Application Service, APP105 Exercise Portal Template Set (Pipeline), APP108 NATO Maritime Availability Database, APP110 Information Environment Assessment. • APP093 Entreprise Architect Application Service, APP095 Agile Tools for Task Management – JIRA Software Service have been added as pipeline services. • INF046 Registration Service has been added as a new customer-facing service for external customers. • The following services have been quantified: PLT006 Database Platform Service, INF020

	DCIS-DCEP Service, SEC012 CIS Endpoint Protection Support Service, SEC021 DCIS – Signal Support Group (SSG), SEC027 Continuous Security Posture Assessment Service. • APP066 Joint Operational Simulation Application Service new flavour added (JTLS Approved Additional Modules service (JTLS_AAM)). • WPS002 Enterprise Identity Access Management Service, DNS Federation flavour added and description updated. • New federated flavour has been added to the following services: APP002 Shared Early Warning Application Service, APP021 JOCWATCH Application Service, APP022 NCOP Application Service new federated flavours • INF044 SEMARCIS/SEMARCOM Deployable Maritime CIS, INF045 DCIS Remote Network Module (RNM), PLT012 Maritime Command and Control Platform (MAR C2P) Service have been moved under the INF035 Deployable CIS Nodes service as flavours. • New flavours added to PLT012-2 Maritime Command and Control Platform (MAR C2P) Service and INF019-2 DCIS – Theatre Liaison Kit (TLK/ILK) Service. • The following PLT008 DevSecOps flavours have been costed: SonarQube, Managed Endpoint, Nexus IQ + Firewall, NATO Trusted Container Registry (Small, Medium and Large), NSF Private Cloud (Small, Medium and Large), NSF Standard Profile, JIRA-only profile, ADO Profile, Gitlab Profile, Power BI profile.
Modification of existing Services	• The names and descriptions of the following services have been revised: APP017 Land C2 Application service, APP019 White Shipping Picture Application Service, APP025 Naval Mine Warfare Support Application Service, PLT015 CQO Reference Platform, SME001 Chief Quality Office Subject Matter Expertise, SME002 Independent Verification and Validation for A2SL, SME012 VeVA CIAV Support service.

	• SME004 Provision of Subject Matter Expertise for the Federated Mission Networking (FMN) Framework, SME009 Provision of Subject Matter Expertise to support the NCS as an Affiliate (NCSaaA) to the Federated Mission Networking (FMN) service descriptions have been revised. • The following services have been renamed: SEC009 Cyber Security Outreach Service, SEC019 Cyber Operations & Exercises, SEC023 Penetration Testing Service, PLT012 Standing Naval Forces Command and Control Platform Service. • The following service descriptions have been updated: APP013 Data-centric Information Services Gateway (DISG) Application Service, APP018 Maritime C2 Application Service, APP059 Joint Exercise and Management (JEMM) Application Service, APP066 JTLS Approved Additional Modules service (JTLS_AAM), APP069 Air Integrated Training Capability (ITC) Application Service, APP070 Training Objective Development and Management (TOMM) Application Service, APP082 Digital Emergency Alert Notification Service, INF038 Deployable Nodes Anchor Service, TRA003 Education and Individual Training Availability and Maintenance, SEC004 Cyber Security Analysis Service, SEC014 Crypto Management and Logistic Support Service, SEC006 Cyber Security Incident Management Service, SEC009 Cyber Security Outreach Service, SEC010 Cyber Security Information Sharing Service, SEC011 Gateway Security Service, SEC019 Cyber Operations & Exercises. • INF036 Deployable SATCOM Service flavour name changed from DART and BBSST to DART and Fast Small. • SME014 Provision of Subject Matter Expertise (SME) to support the Governance and Management of the Vigilance and Enhanced Vigilance Mission Network (VeVA MN) name changed to VeVA SMA and description has been updated. The service rate will be made available in the next CCSC version.

Retired Services	• APP080 Triton Application Service has been retired. • The following PLT008 DevSecOps flavours have been removed: NSF Profile O365E3 (Upgr), Power BI Pro Service and Audio Conferencing. • WPS003-2 Light Profile User has been retired, existing Light Profile users should choose Standard Profile in 2025 service agreements. • WPS008 Entreprise Service Operations Centre has become an underlying service and cost is embedded under WPS001 Managed Device Service, WPS006 REACH Mobile Workplace Service, and WPS016-A Entreprise Managed Mobility Service Smartphone/Tablet (iOS only).

Retired services/flavours

This section includes the services/flavours which have been recently retired and are not available for ordering in this Catalogue release. However, they are still supported for the previous year's quantities, until customers transition to the recommended alternatives or the life expectancy of the service /flavour components reaches its end.

WPS003-2 Light Profile has been retired, existing Light Profile users should choose Standard Profile in 2025 service agreements.

WPS007-2 NONO (NATO Owned NATO Operated) Printer - a device suitable for office or small workgroup environments. It supports up to 5k prints per month, enables up to A4 printing in colour and B/W, and may print up to 20 pages per minute in B/W and 20 pages per minute in Colour.

This flavour is not available anymore for ordering and the alternative is one of the listed Flavours available for ordering (WPS007-1 products). In order to transition to the alternative option, customers need to raise a CRF and the deadline is approximately 14 weeks (including TEMPEST).

Quantities listed in 2022 SLAs/SSPs will be supported until the device has reached its supported life expectancy age (4 years).

WPS016-5 Multi-Factor Authentication Token for Non-managed Devices – This option enables users to access OWA (Outlook Web Access), VDI (Virtual Desktop Infrastructure) or other corporate NU resources made available via the public internet and requiring authentication, through the use of unmanaged (non-NATO) client devices. This One-time-password (OTP) solution - token - is part of the two-factor authentication mechanism required for access.

This flavour is not available for new quantities ordering. Quantities listed in 2022 SLAs/SSPs will continue to be supported.

References

A. C-M(2012)0049, Charter of the Communications and Information Organisation (NCIO), 14 Jun 2012;
B. PO(2015)0394, NCI Agency Customer Funding Regulatory Framework, 7 July 2015;
C. AC/337(FC)N(2017)0025 (INV), Report on Agency Service Costing/ 2018 Service Cost Calculation Methodology, 25 April 2017.

The Catalogue

The NCI Agency Costed Customer Services Catalogue provides a unique and standardised list of Services which are offered to the customer in support of their achievement of specific business outcomes and objectives. The NATO enterprise is complex and extensive; comprised of many different geographically dispersed customers and entities, spanning a wide spectrum of requirements and needs. The NCI-Agency Costed Customer Services Catalogue reflects this complexity by providing a wide range and variety of services, service variations (flavours), value added services, and products. As such, the Costed Customer Services Catalogue forms a true representation of the diverse needs of customers.

The Catalogue constitutes a living document which adapts and matures as customer requirements evolve and change over time. Maintaining a proper alignment between both services and customer requirements is a key principle which enables the NCI Agency to support and add value to customer business. This catalogue has been build and structured on the basis of a customer-centric approach and in accordance with standards and definitions in industry best practice.

The NCI Agency Costed Customer Services Catalogue constitutes primarily a list of Services. However, many of the services in the catalogue can also be offered in the form of a product. To this end, the Agency enclosed a supplemental product catalogue which complements the service catalogue. The product catalogue allows the NCI Agency to remain flexible towards the needs and objectives of customers. Moreover, it provides the means to cater to a larger and more distinct group of customers who, either for technical reasons or business motives, are not able to consume services. The NCI Agency Costed Customer Services Catalogue is therefore comprised of two distinct but paired catalogues, i.e. the Services Catalogue and the Products Catalogue. This introductory note explains the concepts of “services”, “products” and “value added services” for the convenience and understanding of the customer in the use of this Catalogue.

Service

ITIL defines a service as a set of related functions provided by IT systems in support of one or more business areas, which in turn may be made up of software, hardware and communications facilities, perceived by the customer as a coherent and self-contained entity. An IT Service is based on the use of Information Technology and supports the Customer's Business Processes. Additionally, ITIL specifies that an IT Service is made up from a combination of people, processes and technology and should be defined in a Service Level Agreement[1]. In essence, a service delivers an intangible benefit[2], either in its own right or as a significant element of a tangible product. For example, the provisioning of the NCOP functional application service provides customers with an increased situational awareness on the battlespace, increased collaboration and ultimately improved military operations. As opposed to products, the concept of providing a service is not limited to the delivery a specific tangible or intangible system, but rather the provisioning of a whole set of logically related processes, activities, infrastructure, technologies, which in combination with specific skills and knowledge, is able to add value by facilitating customer's business outcomes and goals. Therefore, when we refer to services, we do not just include the provisioning of a specific solution or product, but in addition, include all activities related to the deployment, configuration, management, maintenance and operation. Together, as a packaged whole, they denominate and qualify the concept of a Service. Ultimately, a service provides a level of abstraction, which allows the customer to focus on outputs and outcomes without incurring any intrinsic risks related to the operation and maintenance of the service. When services are priced[3] they incorporate all cost elements which are related to the provisioning of a service (operation and maintenance), both in terms of manpower and external CIS costs.

Services within the NCI Agency Costed Customer Services Catalogue are categorised into 9 different groups, commonly referred to as “Service Portfolio Groupings”, these are:

- Workplace Services
- Infrastructure Services
- Platform Services
- Subject Matter Expertise Services
- Application Services
- Logistic Support Services
- Security Services
- Training Services
- Other Services

Service Portfolio Groupings

Services within the NCI Agency Costed Customer Services Catalogue are categorised into 9 different groups, commonly referred to as “Service Portfolio Groupings”. These are:

- **Workplace Services**: Workplace Services comprise of the basic CIS services that users typically need in their workplace in order to perform their day-to-day business activities, regardless of their job specialization. The majority of NCI Agency’s customer base users consumes these services.

[1] ITIL V3 definition of a Service.

[2] These benefits (outcomes) are generally difficult to measure and quantify and as such are mostly referred to as “intangible”.

[3] NCI Agency is costing or pricing the Services in accordance with the Customer Funding Regulatory Framework.

- **Infrastructure Services**: Infrastructure services deliver the underlying data centre and hardware, software, network, storage and backup functions required for the existence, operation and management of an enterprise ICT environment.
- **Platform Services**: Platform Services provide a package of middleware allowing users to develop, run, and manage applications or data sets without the complexity of building and maintaining the underlying infrastructure. Platform Services deliver the infrastructure and middleware components that enable IT administrators and end users to build, integrate, migrate, deploy, secure, and manage mobile and web applications. Platform Services enable delivery of cost-effective, fully managed operating platforms with expanded, inheritable, and NATO recommended security controls.
- **Subject Matter Expertise Services**: Services provided through a Subject Matter Expert (SME), an individual who is considered an expert on particular subjects, or flagged as an expert in a piece of management software or other technology. The subject matter expert has a particular territory in which he or she has demonstrated above-average knowledge or experience.
- **Application Services**: Software with functionality delivered on-demand to subscribers, which includes web based or client-server applications. Application Services enable customers to collect, manage, present, and distribute information in support of specific Community of Interest (COI) processes. They comprise of entire enabling technology required by any kind of NATO organisations to support a wide spectrum of their business activities.
- **Logistic Services**: The services that support the availability and continuing operation of an asset or piece of equipment in accordance with established standards. Usually, these services entail supply, maintenance, and transportation activities, but may be extended beyond this scope (e.g. calibration, equipment testing, etc.).
- **Security Services**: Services ensuring adequate security of the systems or of data transfers (network and information system security). The Security Services are responsible to NCI Agency for providing support to the development and implementation of Lifecycle security risk management services for NATO ICT IT, IT security related policy and strategy, Leadership in the development of new capabilities and innovation. The security services are focused on to prevent, detect, respond, and recover any IT security related incidents. CIS Security Capabilities provide the secure environment for handling information by CIS components, systems, services, and resources.
- **Training Services**: Services dedicated to educating users on CIS-related topics; designed to help trainees acquire certification in specific areas.
- **Other Services**: Catalogue services that cannot be placed in any other specific Service Portfolio Grouping.
- **NATO Digital Workplace Services**: This is a new portfolio group that captures the services which are part of the NATO Digital transformation roadmap (#One NATO) initiative which is supported by OCIO strategic initiatives.

Service Delivery Lifecycle Stages

A service delivery lifecycle typically follows 3 stages from a business point of view: Service Initiation, In-Service-Support, Lifecycle Refresh. The separation of the lifecycle into these 3 stages facilitates the transparency and management of the different nature of deliverables, time frames and costs that are applicable to each stage. Due to this difference of nature, each stage also has its corresponding separate service rate.

The lifecycle stages and corresponding service rates are explained further below:

1) Service Initiation Rate

Service Initiation is the first stage of the service delivery which corresponds to the one-time cost involved in order for the NCI Agency to set the service up and running.

Service initiation rate covers the cost of procurement of the service assets, delivery to the user location and the initial installation effort for one unit of service requested.

When a customer requests a service for the first time, the one-time Service Initiation Rate is the first rate to be applied. Once the service is initiated, it moves into the next stage: in-service-support.

2) In-Service-Support Rate

In-service-support stage is where service operations and maintenance (O&M) activities are performed by the NCI Agency in order for the service to continue delivering its proposed value.

The in-service-support stage of a service is meant to be long term, and this stage is managed in repeating annual Customer Service Agreements with the customer. In-Service-Support Rate thus corresponds to the annual rate entailing the NCI Agency manpower support costs and the annual fee that the Agency pays to external/industry contracts (license maintenance, 3rd party support, spare parts etc.) for ensuring the seamless continuation of the service provision.

3) Service Lifecycle Refresh Rate

This is the last stage of the service delivery, where the main assets of the service reach the end of their lifecycle and must be replaced for seamless continuation of service delivery. Typically the lifecycle duration is stated in the Customer Service Agreements per service. The service lifecycle refresh rate corresponds to the one-time effort to replace these assets that are at the end of their lifecycle.

The NCI Agency is working towards offering a standard service rate for all applicable services in the Costed Customer Services Catalogue and for each stage in the service delivery lifecycle. The Service Rates section of this Costed Customer Services Catalogue lists the standardised service rates the Agency currently has, with the clear indication of what stage in the service delivery lifecycle the rate applies to. Where the Agency does not yet have a standard service rate, a custom-calculation of the service rate is applied.

Product

As opposed to services, Products are tangible and discernible items, which are delivered as physical assets or intangible assets. While a product is something that can be quantified, a service is less concrete and is the result of the application of skills and expertise towards an identified and specific objective. Most commonly products are delivered in the form of an unmanaged device (e.g. Laptops, desk computers, phones, smartphones, etc.) or software application (e.g. functional applications and specialist applications). Contrary to services, these products will be delivered in a standalone state, without any support in terms of installation, configuration, maintenance and operation. Moreover, especially for functional applications, where the underlying infrastructure is not owned or operated by NCI-Agency. The price for a product therefore equates to its base cost of acquisition. In some instances where standardisation is of no or little importance, i.e. COTS Software, customers are free to purchase the product via their own channels.

Value Added Service

By themselves, products do not satisfy any specific and immediate business need or objective. Only when deployed, configured, maintained and operated they can be used in support of certain business activities. In order to cater for the eventuality where such additional activities are required, NCI-Agency has created the concept of Value Added Services. As the name suggest, value added services enhance and complement specific products, and in some instances services[4]. The product in combination with all or some of its value added services therefore equates to its service counterpart[1]. From a pricing perspective, value added services are mostly, if not exclusively, comprised of costs, which are related to human resources. The cost of a value added service is therefore dependant on the number of manpower units (FTE) that are needed to execute and deliver specific activities. Value added services are referred to as services because they exclusively consist of the delivery of specific NCI-Agency expert skills and knowledge. They are however quite distinct from the services which were defined earlier. Therefore, the NCI-Agency Customer Service Catalogue will group all of the value added services in a separate list in the future.

Value added services can be provided for a number of areas or activities:

- Installation & Configuration
- Release Management (Patch and version releases)
- In-Service-Support (Level 1,2 and 3)
- Mentoring
- Training
- Project Support
- Auditing

[1] It should be noted that in some instances, as for example with mentoring and training which qualify as “value added service”, customers who have opted for the service are still eligible to purchase these value added services.

Service & Product Attributes

The NCI Agency Costed Customer Services Catalogue adopted a standardised template for describing services and products. A description comprises a specific set of attributes, which define and qualify the service or product. The description templates have been designed from a business- and customer-centric point of view. The following table lists and defines all attributes valid for NCI Agency Product and/or Service.

#	Attribute name	Attribute Description
1	Service/Product ID code	6 character code, which uniquely identifies a service or product; customers can use this code to refer to specific service or product; provided by NCI Agency Service Portfolio / Service Catalogue Management (COO BPM SPCM).
2	Service/Product Name	Name designating the service or product, as proposed by the Service Owner.
3	Portfolio Group	Indicates the Service Portfolio Group to which the service in question belongs: Application, Infrastructure, Platform, Subject Matter Expertise, Security, Training, Workplace, Other.
4	Service/Product Status	Indicates the Portfolio status of the Service or product, i.e. “Pipeline”, “Available” or “Retired”. Pipeline services are planned to become available, and may even be partially available to specific customers. Available services are offered to customers as defined in the Catalogue. Retired services are not available for ordering, but they might be fully or partially supported for a specific period of time after being announced as retired through the Catalogue.
5	Service/Product description	Describes the service or product from a non-technical perspective.
6	Value Proposition	Explains in business terms how a service or product supports specific business processes and as such facilitates specific business outcomes and objectives.
7	Service/Product Features	Lists and describes the features of the service or products. Complements the service description.
8	Service/Product Request	Describes the procedure, which is required for customers to request the service or product. Describes the means by which customers can report incidents and problems related to the use of the service or product.
9	Service/Product Flavours	Describes the different variations in which a service or product can be offered.
10	Available Networks	Lists the security environments in which the service or product is available, i.e. NU – NU – NS – MS, on which the service can be delivered.
11	Service/Product Prerequisites	Lists the services, which are required beforehand in order to consume the service in question. The Customer needs to ensure that the prerequisite service are in place. For products, this section will be dedicated to system prerequisites.

#	Attribute name	Attribute Description
12	Standard Service Support levels	Details the availability target for the service, i.e. the time the service is available to the customer considering the potential downtime of a service. This figure does not include any maintenance activities. Service Availability Target is expressed in terms of the minimum "Monthly Uptime Percentage" time frame. Percentage availability is calculated by the following formula: % Availability = 100 x (Available Minutes* - Downtime) / Available Minutes **Minutes available during agreed reporting period excluding planned maintenance minutes* This section also details the restoration time for a service, i.e. the maximum time which is needed to restore the service in the eventuality of a major or critical incident.
13	Service Reporting	Details the standardised service reporting which is provided as a deliverable of each service
14	Support Hours	Details the times during which helpdesk support (including level 2 and 3 support) is available for the customer.
15	Service/Product Cost	Describes the unit of measure (service unit)[1] used in the calculation of the service price/rate. Provides reference for price detail, or describes specific application of the service rate, where applicable. This attribute will only detail the base acquisition price for products.

Unless otherwise specified in a specific service definition, the following attributes are equally valid for all services in the Catalogue:

Service Status: Available

Service Support levels and Prioritization: All services have default P4 priority. Any change of priorities is subject to specific stipulations of the respective service definition within this Catalogue and relevant service provisioning agreements (Service Level Agreements and/or Service Support Packages).

The service rates reflect the prioritisation requirement of the services based on the default priotisation in the CCSC plus the ACO ABIPAT tables in SLAs.

[1] Currently, the NCI Agency applies specific unit of measure for only a portion of the overall service portfolio. These are referred to as "unitized" services, as opposite to majority services that are "non-unitized", and have the unit of measure defined as 1. Non-unitized services are priced per total cost of the specific service delivery, and normally funded by one funding mechanism (one service provisioning agreement). In cases where those services are provided to both External and Internal Customers, price for each specific service delivery other than the main one needs to be separately defined in the process of the service provisioning agreement development. Prices for unitized services are equally applied per unit of measure for all customers.

Support Hours:

- Centralized Service Desk specialist agents are available Mon-Thurs 06.00-22.00 CET, Fri 06.00-20.00 CET. Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.
- Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time).

Service Requests

- **New Service Request:**

  Please complete Customer Request Form and contact NCI Agency, as defined within the form.

- **Incident/problem reporting:**

  Contact Centralized service desk: 626 3177 (NCN) or the commercial numbers:
  Belgium +32 65 44 3177,
  Netherlands +31 70 374 3177,
  Italy +39 081 721 3177,
  Germany +49 282 4978 3177,
  NATO HQ +32 02 707 5858.

NCI Agency Education and Training Services

NCI Agency provides a comprehensive catalogue of NCI Agency Education and Training Services covering in the entire spectrum of NATO-Specific C4ISR and Cyber, including user, administrator and technical training, as well as courses for military and civilian staff working in more general Communications and Information Systems posts. The Catalogue also explains how to obtain services, the procedure for seat allocation as well as the pricing policy and prices for many of the courses. The catalogue is a living document, as the Agency dynamically adjusts its course offerings to accommodate new systems being delivered, systems being phased out, new versions and changing customer requirements. The catalogue and pricing information can be found at www.ncia.nato.int/training.

NCI Agency Services not covered by the Costed Customer Services Catalogue

The Agency aims to offer its services, to the greatest extend, in a standardized manner via the Agency Costed Customer Services Catalogue (CCSC), where each Service has a standard scope of service provision and Standard Service Rate (where applicable). The use of the CCSC services provides both the customers as well as the Agency elements a pre-defined standard understanding of the scope, expectations and deliverables for the customer needs.

However, in cases where a local support is required by a customer that cannot be attributed to a CCSC Service, the Agency provides the flexibility to offer these service offerings through a group of what is called: 'Non-Catalogue Services'. Agency provides a variety of support for its customers under the scope of 'Non-catalogue service', however for practicality, the Agency groups these services under one of its **9 Non-Catalogue Service** titles (please see table below) during reporting. In that regard, these 9 service titles rather represent a Service Group, rather than a standard offering. Because the scope of each service for these services is different for each customer, the specific service deliverables for these services should be documented in the corresponding Service Agreements..

The management and provision of these Non-Catalogue Services are handled by local Agency elements. Financially, the cost of these services are custom calculated and agreed during the Service Agreement negotiations between the customer and Agency.

In the table below, you may find an explanation of what each Non-Catalogue Service, or service group can entail.

NCI Agency Non-Catalogue Services		
Title	**Service ID**	**Description**
Local Audio / Video Support Service	LEG001	Corresponds to local audio visual support that is not part of a standard service offering in the CCSC. May include but is not limited to operation and maintenance of projection systems, TVs, IPTV, portable audio systems, large screen displays (ex Videowall) and smart boards.
Local Internet Access Service	LEG002	Corresponds to locally managed fixed or wireless internet access services that are outside the scope of the standard service offering (Enterprise Internet Access Service – INF003) found in the CCSC.
Local Transmission Service	LEG003	Corresponds to locally managed and supported transmission lines for connecting NATO networks to/from the site that are not covered under the CSLA funded transmission services (INF014)
Local Applications Service	LEG004	Corresponds to any local application maintenance and support requirement that is not part of a standard service offering in the CCSC, where the application will be locally managed.
Local CIS Security Service	LEG005	Corresponds to local CIS Security support requirement that is not part of the centralized Agency service offerings or where the customer requires local SME and consultancy support on matters related to CIS Security.
Local Radio Communication Service	LEG006	Corresponds to local Radio Communication requirements (like first responder radio equipment) that is not part of a standard service offering in the CCSC.
Local SME / PoW Service	LEG007	Any local Subject Matter Expertise requirement that customers that is not part of a standard service offering in the CCSC. The scope of services ranges from providing SME and consultancy services to

		supporting customers on PoW related activities such as Small Value Sales.
Local Other Service	LEG008	Any local support requirement that doesn’t fall under neither of the categories above.
Local User Training Service	LEG009	Local training requirements of the customer that are beyond the scope of the NATO CIS School that is covered in the CSLA.

NATO Communications and Information Agency

Costed Customer Services Catalogue - Definitions

This page is left blank intentionally

.

Workplace Services

This page is left blank intentionally

WPS001 Managed Device Services

Service ID: WPS001

Service Name: Managed Device Service

Portfolio Group: Workplace Services

Service Description: The Managed Device Service provides the users with a client device[1] (of various form factors) that allows them to secure a connection to NATO networks (in a specific security domain). The service includes full office automation software[2] (Microsoft Office Professional Suite), Windows operating system and NATO mandatory security tools. The service also includes a flavour for non-NATO network attached (i.e. standalone) devices.

Value Proposition: The service offers a managed device, which will enable the connection to access NATO CIS resources (office automation, browsing and access to applications). This facilitates operational efficiency and effectiveness and supports all business processes throughout the NATO enterprise.

Service Features: The software baseline includes a Windows operating system, primary and secondary internet browser, a PDF reader, NATO recommended security tools (including controlled access to peripherals). For fully approved (A2SL tested) COTS applications the labour element of packaging, patching and deploying such applications is included. The service excludes the procurement of new hardware devices (laptops, desktops, thin clients, monitors, mouse, keyboard, webcam and headset, KVM or any other accessories). This service equally excludes the life-cycle replacement of obsolete equipment as well excludes the testing and approval efforts for COTS applications.

Service Ordering and Request: The new service instances are requested by submiting a Customer Request Form (CRF).

After a service is initiated, the in-service support phase for the service is managed through annual Service Agreements with each customer.

The service fee for this service is charged to each Agency customer directly, meaning the service charges are not covered by the NATO central funding channels for NATO, therefore each customer requests/orders this service directly themselves.

For IT Incidents, Request for Information (RFI) and Service Requests (SR) regarding this service, the Enterprise Sevice Operations Centre (ESOC) is the NCI Agency's Single Point of Contact (SPOC) for all eligible Customers and Users.

[1] Please see Service Cost/Price paragraph and Service Delivery Lifecycle Stages section for the lifecycle stages of a service along with the corresponding deliverables and the service rates applicable in each stage.

[2] Please note that the license component of MS Office Professional should be acquired through the WPS003 Enterprise User License service, hence WPS003 is listed as a prerequisite to this service. A license can serve multiple managed devices, therefore it is not integrated into scope of this service.

Service Flavours:

WPS001-A Static Desktop (Workstation) Device - This device is a workstation that needs to be connected to a wired network. It features an external monitor (minimum 24”), keyboard and mouse. In exceptional cases, a thick client may be provided as a standalone device as long as all security requirements are met. As option (subject to a separate funding agreement), an additional Monitor, a VTC camera, a headset and a KVM can be provided. Static Desktop Devices are no longer used at NATO Unclassified level unless required by specific performance based applications. For standard NATO Unclassified usage, please see Portal (Laptop) Device service flavour.

WPS001-B Thin Client Device - This device is a computer that runs from resources available on a central server instead of a local workstations. Thin clients work by connecting remotely to a server-based computing environment where most applications, sensitive data and memory are stored with the need to be connected to a wired network. It features an external monitor (minimum 24”) keyboard and mouse. As an optional extra (subject to a separate funding agreement), an additional Monitor VTC camera, a headset and a KVM can be provided.

WPS001-C Portable (Laptop/Tablet[1]) Device - This device can be connected to a wired network or to a wireless network. It comes with an external power adaptor, external mouse and a USB-C docking station. In exceptional cases, a Portable client may be provided as a standalone (NU, NR, NS) device as long as all security requirements are met.

Note: The WPS001-C Portable (Laptop/Tablet) Device, can connect to NCI Agency supported CIS (NU/NR) through various connectivity:

- Static connection, i.e. cabled connection to an existing NU network(Wifi or cellular disabled)
- Remotely through either WiFi or cellular connectivity .

If connected *only* via static connection to NU network port, the laptop device will be considered equivalent to the WPS001-A Static Desktop (Workstation) Device service flavour and hence the WPS016-C (Enterprise Managed Mobility Service NU/NR) service charge is not applicable.

In case the WPS001-C Portable (Laptop/Tablet) Device has its WiFi or cellular capabilities enabled, the device is enabled for remote connectivity and hence the WPS016-C (Enterprise Managed Mobility Service NU/NR) service charge applies. For this device type there is an optional rate to include the service lifecycle (obsolescence) refresh.

Available on:

Static (Workstation) Desktop and Thin Client device:

[1] Tablet with Windows OS only.

NATO Unclassified [exceptional circumstances only - for example cartographic workstation]
NATO Restricted [exceptional circumstances only - for example cartographic workstation]
NATO Secret
Mission Secret
Standalone device (not connected to any NATO network) [exceptional circumstances only]

Portable (Laptop) Device:

Standalone device
NATO Unclassified
NATO Restricted
NATO Secret [exceptional circumstances only]

Service pre-requisites:

INF001 LAN Service (not applicable to standalone device)
WPS002 Enterprise Identity Access Management Service (not applicable to standalone device)
WPS003 Enterprise User License Service
WPS008 Operations Centre Service

Service lifecycle for device:

The below table shows the life expectancy per device category , the service owner shall inform the entity utilising the device before life expectancy reaches within a suitable time frame.

Service Component	**Life Expectancy**
VDI Clients	6 Years
Desktop/Workstation clients	5 Years
Laptop/Tablet Clients	3 Years

Standard service support levels:

Service Availability[1] Target: 99.0%

Standardised time to deliver new service instance[2]: 3 working days (installation and configuration of new managed device)

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

[2] Provided the underlying CIS infrastructure (INF001; INF002; INF014) is ready and devices are on site

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full priority resolution times and generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency SLA, SSP or any other agreement with the Customers.

Service Reporting:

ACO/ACT Customers: The standardised service reporting is provided as a deliverable of this service. ACO standardised reporting templates are listed in the SLA Annex 18 and managed by ACO KPI/KQI WG.

Quarterly Reports:

Impact on service availability and service performance reports at Service Access Point (SAP) (via incidents)

Incident management report base on ITSM tickets and trend analysis

Change management and ASI report based on ITSM tickets

CIS Security and Cyber report

Asset and Configuration Management reports

Additional service reporting requirements can be requested through the respective SLAs which are subject to NCIA's cost and feasibility assessment.

Service Cost / Price: The unit of measure for the service is per device. Price details available on request. The service rate currently published in the CCSC reflects the service in support rate (O&M rate) which does not represent the full end to end cost of the service. For customers who are procuring new quantities of the service the service initiation (procurement and deployment of the service components) shall apply, also for components which reaches the end of life phase the service lifecycle refresh rate shall apply. Both the service initiation and service lifecycle refresh rates are not standard rates (except for NATO HQ). As a pilot phase, the obsolescence refresh option is now made available for WPS001-C Portable (Laptop/Tablet) Device.

WPS002 Enterprise Identity Access Management Service

Service ID: WPS002

Service Name: Enterprise Identity Access Management Service

Service Type: Enabling Service

Portfolio Group: Platform Services

Service Description: The Enterprise Identity Access Management Service (E-IDAM) provides identities (including provisioning and de-provisioning of User Accounts, Privileged Accounts, Service Accounts, Computer Accounts), and the capability to share trusted identity information between different domains and to Enterprise users. The information on identities retrieved from different authoritative sources. Additionally, the service includes the provisioning of personal storage space (minimum 20 GB) for storing personal information and documents (only for WPS002-1A: User Account on-premises).[1]

The Service allows controlled access based services. The access services can be available across domains utilising AD-Federation. It offers a Single Sign On experience for users with a valid NATO Enterprise Identity. The service also provides Directory Synchronization enabling Global Address List synchronisation to the NCI Agency External Customers, Mission environments, and Allied Nations.

The Service provisions, operates, maintains, retires authentication subsystems like LDAP, Domain Controllers, Active Directory, ADFS, MIM, SSO. The service can delegate limited authority to the supporting elements.

Value proposition: E-IDAM provides value to customers through the hosting and sharing of identity information across multiple identity stores, improving data quality and reducing the administrative burden for connected systems. This ensures a coherent set of identity data from authoritative sources, while increasing the security posture of the NATO Enterprise.

The Service provides access to the Alliance GAL, including structured contact information. It enables searching for people and groups somewhere in the Alliance.

The Service allows the users to securely access different NATO networks, and it enables the NCI Agency to manage and maintain the access to the identities to track and control usage of resources ensuring only authorized users are accessing relevant services/resources. Furthermore, it enables enhanced security, prevention of oversubscription to the services.

Service Features:

Identity Management shared information across multiple identity stores, improving data quality and reducing overhead for connected systems. Identity information can be synchronised between different affiliates, supported by automated workflows and enables account provisioning and de-provisioning. Data sources/consumers can use native interface of E-IDAM to retrieve or modify it through industry standard protocols

[1] The NCI Agency is assessing this statement as it is not aligned with the current capability of the underlying central storage service and might be subject to modification in the following catalogue releases.

and mechanism (like LDAPs). Moreover, Lifecycle management (from provisioning to de-provisioning) of Identity and its attributes is being provided with E-IDAM.

Access Management is available for the compatible services requiring authentication for users and/or resources. The access management (authentication/control/validation) is provided by credential management, security group memberships, and policies (like GPO), also through integration with NATO PKI.

Account Lifecycle Management provisioned and managed on-premises and off-premises (cloud) by WPS002 including the secure and sanitized environment. The accounts on the cloud requires additional licenses to reach and consume cloud resources, as well as security & safety requirements dedicated to the cloud provider, also it brings efficiency with automation by nature of cloud.

Web Federation provides cross-domain authentication to reach web-based resources seamlessly (SSO) to increase the user experience and to enable the secure service on Windows based ADFS.

DNS Federation - distribution of domain name system (DNS) authority across multiple, independent entities or organizations (i.e. nations, partners) to enhance resiliency, scalability and diversity within the DNS ecosystem, reducing the risk of single points of failure and promoting decentralization.

Data Directory Synchronization (DDS) is provided through a number of directory synchronisation servers, which are inter-connected to identity directories of the participating NATO organisations and Nations. The DDS allows the exchange of shared identity information (such as Display Name, Organisation Name, E-Mail Addresses and other relevant contact information) between service subscribers. GAL Sync is a flavour of the Data Directory Synchronization.

Service Flavours: The Service is available in multiple flavours, with the following options:

1. **WPS002-1 User Account (On-premises or Off-premises)**: Per account

Personal Data Protection deliverables below are included within this flavour (Accounts Lifecycle Management).

- Service Support
  - Inventorying personal data.
  - Data Catalogue expansion to include PDP identification and Stakeholder data with PD elements.
  - Support Stakeholder PD information requests and solutions.
  - Incident management.
  - Coordination of response preparations with Stakeholder PDPOs, Cyber, etc.
  - Dispute resolution and mediation process.
  - Legal on implementation, incident management and dispute resolution.

- Training
  - SME support to NATO training sponsored by OCIO and developed by Agency/Academy.
  - PDPO training coordination.
  - Additional PD Training time required for PDPO office, Data Processers, Controllers, Owners and Stewards.
  - Training support sessions from PDPO to same audience (e.g. SDMs for systems with Stakeholder data).
- Capabilities: Personal Data Inventory and Dependent Catalogues
  - Implement and maintain Personal Data Inventory of Stakeholder and NCIA PD.
  - Acquire or build capabilities, including increased developer ours for inbuilt solutions.
  - Implement and maintain Data Catalogue that includes Stakeholder and NCIA* PI Data elements.
  - Implement and maintain Process Inventory that includes Stakeholder and NCIA* PI Data elements.
  - Implement and maintain ICT Privileged User List s Inventory that includes Stakeholder and NCIA* PI Data elements.

2. Federation:

A. **WPS002-2A Web Federation**: Per connection.

B. **WPS002-2B DNS Federation**: Per connection.

3. Data Directory Synchronization

A. WPS002-3 GAL Synchronization: Per connection.

Service Ordering and Request: There is no specific service initiation cost associated with "Account" flavour, and the new service instances are requested and created by submitting standardised service request (work order) through the ITSM toolset. For "Web Federation" and "DDS-GAL Sync", customers should initiate a CRF since there is initiation cost associated with.

All exceptions to the service instance calculation method will be agreed between the Provider and the Customer and documented in the individual SLAs/SSPs accordingly.

Service Reporting:

ACO Customers: The standardised service reporting is provided as a deliverable of this service. ACO standardised reporting templates are listed in the SLA Annex 18 and managed by ACO KPI/KQI WG.

Quarterly Reports:

- Impact on service availability and service performance reports at Service Access Point (SAP) (via incidents)
- Incident management report base on ITSM tickets and trend analysis
- Change management and ASI report based on ITSM tickets
- CIS Security and Cyber report
- Asset and Configuration Management report

Additional service reporting requirements can be requested through the respective SLAs which are subject to NCIA's cost and feasibility assessment.

Available on:

NATO Unclassified

NATO Restricted

NATO Secret

Mission Secret

NATO Partner network

Public Cloud (limited with Security conditions)

Service Prerequisites:

INF002 NATO Network Point of Presence

INF003 Enterprise Internet Access Service

INF004 Infrastructure Virtualization Service

INF005 Infrastructure Integration Service

INF016 Infrastructure Back-up and Archiving Service

PLT006 Database Platform Service

SEC011 Gateway Security Service

Standard Service support levels:

Service Availability[1] Target:

For service flavour "Account LM":	99.0%
For service flavour "Federation":	99.9% during Support Hours
	99.5% outside of Support Hours
For service flavour "DDS":	99.0%

Standardised time to deliver new service instance: 1 working days[2] (creation of new account)

Service Restoration: Where the service deems unavailable, the service restoration period for a critical incident:

For service flavour "Account LM":	4 hours
For service flavour "Federation":	1 hour during Support Hours

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated based on the followings:

- "Available Minutes": during agreed reporting period excluding planned maintenance minutes
  (Available Minutes - Downtime) / Available Minutes x 100

[2] Taking into consideration that all required documentation is provided to ESOC

	4 hours outside of Support Hours
For service flavour “DDS”:	48 hours [1]

Service Cost / Price: The unit of measure for the service varies depending on the flavour. For the flavour “Accounts” the unit of measure is “per User Account”, for the two other flavours the unit of measure is “per Connection”.

Please see Service Rates document for standard rates applicable to the service.

1- Accounts Lifecycle Management
User Account (On-premises or Off-premises): Per account

2- Federation:

A. Web Federation: Per connection

B. DNS Federation: Per connection

3- Data Directory Synchronization (GAL-Sync): Per connection

[1] Already synchronised objects will remain as available to end-users.

WPS003 Enterprise User License Service

Service ID: WPS003

Service Name: Enterprise User License Service

Portfolio Group: Workplace Services

Service Description: The Enterprise User License Service provides a Microsoft Enterprise User License based on NATO User Profile which comes in three pre-packaged profiles (NATO light,NATO Standard and NATO Delegation User) of which all three contain the same licensing components and the same functionality to the user, however with different number of qualified devices that the licenses are allowed to run on.

Value proposition: This service allows users to access via multiple devices (desktop, laptop, thin clients…), on multiple networks (business, operational, missions & exercises), and also to leverage the mobile devices that are increasingly typifying our environment (phones, tablets, iOS, Android). This user approach achieves both of the aims of reduced cost, and simplified licensing and management.

Service Features: The key licensing components cover the core business needs of the users for Windows, Office and server access across the NATO Enterprise. The licensing components included are:

- Windows: Windows Software Assurance per user provides access to Windows Enterprise for install or VDI across devices
- MS Office: On-premise version of MS Office Professional Plus Suite across Windows devices
- Enterprise Client Access: enterprise client access licenses to access the server functionality in Windows, Exchange, SharePoint per user across devices
- SQL Client Access: Client access to SQL Server per user across devices
- Skype for Business Plus Client Access: Client access to enterprise-grade instant messaging and phone features in Skype for Business per user.

Service Flavours: The Enterprise User License Service is available in the following flavours:

- **WPS003-1 NATO Standard Profile** authorizes use of the licensed Products on **up to 5 (five)** Qualified Devices on each network.
- **WPS003-3 NATO Delegation User** authorizes the use of the Product on a **single** Qualified Device by **up to 8 (eight) users** where the Software is installed (i.e. delegations, NMRs, third party).

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

Service prerequisites:

None

Standard Service support levels: N/A

Service Cost / Price: The unit of measure for the Service is Per User or Per Device, depending on the flavour. Please see Service Delivery Lifecycle Stages section for more information about the general overview of the type of deliverables involved in each stage and the scope of corresponding service rate.

Please see Service Rates document for standard rates applicable to the service.

WPS004 E-mail Service

Service Retired and consolidated under WPS012 – Workstream Collaboration Service.

WPS005 Instant Messaging and Collaboration Service

Service Retired and consolidated under WPS012 – Workstream Collaboration Service.

WPS006 REACH Mobile Workplace Service

Service ID: WPS006

Service Name: REACH Mobile Workplace Service

Portfolio Group: Workplace Services

Service Description: The REACH Mobile workplace Service provides client devices (Laptops) that allow to connect to the NATO Restricted network.

Additionally, the Service includes:

- A User Account, Password and PKI token to access the NR.AIS Network (WPS002);
- A mailbox on the Restricted network (WPS012); and
- An IM Collaboration Account (WPS012).

The Laptop Client device is loaded with the office automation software (MS Office Professional Suite), Windows operating system, VPN client software, and security and management tools.

Value proposition: The REACH Mobile workplace service is a bundle of four customer-facing services (Managed Device Service, Enterprise Identity Access Management Service, E-mail Service, IM collaboration Service), infrastructure and platform services, offered as a single service package for the NATO Restricted Network.

Service Features: Same as the four individual services comprised in this service offer. There is an additional option for a Static work position which consists of a docking station, dual LCD Monitor, VTC camera, Keyboard and mouse. (This option is only applicable for the Portable Client Device service flavour).

Service Flavours:

Portable Client Device (Laptop) – provides a Laptop device that needs to be connected to a wired or wireless network. The laptop comes with a power supply, a carrying case, a headset, and an external mouse.

Optional Static Work position – only applicable for a portable client device service flavour; provides a docking station for the portable device, dual LCD monitors, a VTC camera, a keyboard, and a mouse.

Available on:

NATO Restricted

Service Prerequisites:

WPS003 Enterprise User License Service
WPS008 ESOC Service – mandatory service for each WPS006 device.

Standard Service support levels:

Service Availability Target : 99.0%

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

Service Cost / Price: Unit of measure used for service quantification is Per Device.

Please see Service Delivery Lifecycle Stages section for the lifecycle stages of a service along with the corresponding deliverables and the service rates applicable in each stage.

Please see Service Rates document for standard rates applicable to the service.

WPS007 Print/ Scan/ Copy Service

Service ID: WPS007 (version 2023)

Service Name: Print/Scan/Copy Service

Portfolio Group: NATO Digital Workplace Services

Service Description: The Print/Scan/Copy Service includes the management of multifunctional devices (MFDs), i.e. devices with combined print, scan and copy functionality, as well as document management and workflow solutions to improve an organization's printing environment. The Print/Scan/Copy service enables the user to create hardcopies of digital content or to digitise hardcopies.

Under this service, NCI Agency uses a large framework contract with a global supplier of multifunctional devices to ensure standardization, and service reliability across the Alliance at the most efficient price.

These multifunctional devices are by default enabled with badge-controlled authentication and can be acquired in various TEMPEST tested variants.

Depending on the service flavour selected, lifecycle replacement after five (5) years is included at no additional cost to the customer[1].

Value proposition: The Print/Scan/Copy Service supports various Business Processes across the Enterprise by performing multiple office imaging tasks, such as input, output and transmission of documents. It allows electronic content to be re-produced in hardcopy for easy reading, commenting, obtaining physical signatures, etc. The service also allows physical paper content to be electronically stored and transmitted to relevant recipients on NCI Agency supported system.

Service Types: The Print/Scan/Copy service includes four service flavours[2]:

WPS007-1 – A: A3 Large Print Volume MFD (ImageRunner Advance DX C5840)

This printer comes with the following technical specifications:

- 40 ppm
- Optimum print volume: 5.000 – 30.000 per month
- Lifetime 2.000.000 prints
- Color & B&W Printing/Scanning/Copying
- Double-sided Printing/Scanning/Copying
- Document Feeder for scanning of multiple documents
- Scan directly to users' email address
- Multiple paper sizes possible: A3-A4-A5-A6-Envellopes
- User Identification through RFID card

[1] One-time cost related to TEMPEST testing is not including in the five (5) year service rate.

[2] Exact MFD device models can change without prior notification due to contractual changes and/or end of service notifications from current supplier.

WPS007-1 – B: A3 MFD (CANON ImageRUNNER ADVANCE DX C3830i)

This printer comes with the following technical specifications:

- 30 ppm
- Optimum print volume: 5.000 – 10.000 per month
- Lifetime 1.000.000 prints
- Color & B&W Printing/Scanning/Copying
- Double-sided Printing/Scanning/Copying
- Document Feeder for scanning of multiple documents
- Scan directly to users' email address
- Multiple paper sizes possible : A3-A4-A5-A6-Envellopes
- User Identification through RFID card

WPS007-1 – C: A4 MFD (CANON imageRUNNER ADVANCE DX C357i)

This printer comes with the following technical specifications:

- 35ppm
- Color & B&W Printing/Scanning/Copying
- Double-sided Printing/Scanning/Copying
- Document Feeder for scanning of multiple documents
- Scan directly to users' email address
- Multiple paper sizes possible : A4-A5-A6-Envellopes
- User Identification through RFID card

WPS007-1 – D: A4 Desktop-sized MFD (CANON i-SENSYS X C1333i)

This printer comes with the following technical specifications:

- 33ppm
- Color & B&W Printing/Scanning/Copying
- Double-sided Printing/Scanning/Copying
- Document Feeder for scanning of multiple documents
- Scan directly to users' email address
- Multiple paper sizes possible : A4-A5-A6-Envellopes
- User Identification through RFID card

WPS007-1 – E: Plotter (Large Format Printer)

Traceability with previous service flavours (CCSC 7.1):

Old flavour (CCSC 7.1)	Old flavour name (CCSC 7.1)	Mapping to new flavour

WPS007-1	COCO MFD (Contractor Owned Contractor Operated Multifunctional Device)	WPS007-1 - A: Large Print Volume MFD WPS007-1 - B: A3 MFD WPS007-1 - C: A4 MFD WPS007-1 - D: A4 Desktop-sized MFD
WPS007-2	NONO (NATO Owned NATO Operated) Printer	Service Flavour is not available for new quantities ordering Existing quantities listed in 2022 SLAs/SSPs will be supported until device has reached its supported life expectancy age (4 years)
WPS007-3	Plotter (Large Format Printer)	WPS007-E: Plotter*
WPS007N-1	Division Printer (MFD)	WPS007-B: A3 MFD
WPS007N-2	Workgroup Printer	WPS007-C: A4 MFD

*** Note:** Due to the limited quantities of plotters within NATO, and their specific usage, this service flavour is not available as part of the large framework contract. The service is offered with a Service Initiation cost and annual service rate calculated upon request.

Standard Service Features: The Print/Scan/Copy Service provides the following *minimum* features:

- Grey-scale and Colour printing
- Singe and Double-sided printing (paper size various according to service flavour selected)
- Document feeder for scanning of multiple documents
- Scan directly to user's email address
- Paper Input Trays supporting multiple paper sizes
- Copy functionality, single and duplex sided
- Toner and toner electronic advanced notification for replacement
- User authentication through scanning of RFID card (typically AMIS badge)

Additional (optional) Service Features (Applies to Service Flavour A and B only):**

- Stapler finisher
- Booklet finisher
- High-volume document feeder

- Hole Puncher – 2 or 4 hole

Please note, that any optional features needs to be selected up front at service initiation stage and cannot be deselected throughout the duration of the service commitment.

**** Note:** For MFDs used on high-side (NS/MS), any optional features need to be requested at the service initiation stage, and it is not possible to have optional features retrofitted due to the mandatory requirement for TEMPEST testing of the MFDs.

Available on:

NCI Agency supported CIS on both low side (NU/NR) and high-side (NS/MS).

Please note: For MFDs used on the high-side (NS/MS), TEMPEST testing of each MFDs is mandatory. The cost for TEMPEST testing is a one-time only cost which will be included in the Service Initiation cost. The Annual Service rate for both TEMPEST and non-TEMPEST tested printers remains the same. The standard delivery time is 14 weeks (including TEMPEST).

Service prerequisites:

WPS001 Managed Device Service (or qualified connected device)
WPS002-1 Enterprise Identity Access Management Service - User Access Account
WPS012 Workstream Collaboration Service (for scanning functionality only)

Standard Service Support Levels:

General service availability* target is 99.0% with Priority Resolution Times and Generic Service Priority Assignment Matrix in accordance with the NCI Agency standardised Service Level Agreements in force.

- Standard Support: 08:30 - 17:00 (included in standard service rate)
- VIP Support: 06:00 - 22:00 (service rate available upon request)
- VVIP Support: 00:00 - 23:59 (i.e. 24/7 support) (service rate available upon request)

***** Only if one of the following conditions are met, the service will be considered unavailable:

1. Service is unavailable to all users in an organisation. For example users are unable to select the print queue while attempting to print, or the entire print capability is unavailable.

50% or more of the MFDs deployed in a single geographical location are unavailable. Unavailability of more than 50% of deployed MFDs in a single geographical location.

For ACO/ACT customers: Incident prioritisation and service restoration requirements are in accordance with the Aligned Baseline Incident Priority Assignment Table (ABIPAT) agreed in the SLAs. Service Request / Request Fulfilment prioritisation and service installation requirements are in accordance with implementation time targets agreed in SLAs.

Service Cost/Price:

The unit of measure, used for service costing is per Multi-Functional Device[1] and per type of printed page.

The exact service rate is not yet calculated, but is estimated due to ongoing renewal of the active contract with current supplier. For 2024 budgetary purposes the following annual service rates are recommended to be used***:

******* The service rate is based on a full five-year service commitment. In case of shorter service commitment, the investment cost of the MFDs will be borne at service instantiation. The annual service rate will equally be lower depending on the length of the service commitment decided. Exact service rate calculation will be provided at price proposal stage.

Please see Service Rates document for standard rates applicable to the service.

Service Reporting:

ACO/ACT Customers: The standardised service reporting is provided as a deliverable of this service. ACO standardised reporting templates are listed in the SLA Annex 18 and managed by ACO KPI/KQI WG.

Quarterly Reports:

Service availability and service performance reports at Service Access Point (SAP) (via incidents)

Incident management report base on ITSM tickets and trend analysis

Change management and ASI report based on ITSM tickets

Additional service reporting requirements can be requested through the respective SLAs it may be subject to additional service fees.

[1] For new entities, not already consuming the WPS007 Print/Copy/Scan Service, there is a one-time cost of EUR 7,200. This covers the instantiation of the backend required plus socialization efforts enabling an effective use of the service.

WPS008 Enterprise Services Operations Centre

Service Name: Enterprise Services Operations Centre (ESOC) Service

Portfolio Group: Workplace Services

Service Description: The Operations Centre Service is the 24/7 NCI Agency's Single Point of Contact (SPOC) for all eligible Customers and Users. it offers up to level 2 support on IT Incidents, Request for Information (RFI) and Service Requests (SR) for all NCI Agency provided Services.

Value Proposition: The Service provides continuous monitoring, response, control, and operational reporting capabilities for the NCI Agency's operated CIS infrastructure and services to support network integrity and end-to-end service delivery coherence. Sustained by mature ITIL Service Operations best practices, the Service enables the exercise of the command and control over all service assets ensuring service delivery is in accordance with all contracted service provisioning agreements (SLAs, SSPs, MOUs, POW, etc.). Furthermore, the Service enhances the ability to avoid IT services degradations and/or interruptions minimizing the impact on User Communities by proactively taking actions on identified disruptive service events. The Service provides efficiencies in terms of overall costs of service delivery and reducing Incident/Request resolution times through centralized management. The full range of the Agency's support capabilities will be available via a single point of contact, which serves as key stakeholder on maintaining strong liaison with customer communities in order to resolve Incidents prioritization conflicts, coordinate service outages and escalate / notify hierarchically and functionally critical incidents as deemed necessary and agreed-upon.

Service Features: The ESOC Service is based on the proficiency, combination, and coordination of five main elements: the Centralized Service Desk (CSD), the Network Control Centre (NCC), the VTC Control Centre (VCC), the Service Support Centre (SSC) and the Duty Control Officers Team distributed across two distinct geographical locations to ensure Service resiliency.

(Please note regarding the VCC element that VCC is listed for information purposes in the paragraph above to describe all the elements that lie within ESOC as an entity, however in accordance with the service-oriented principles of the catalogue VCC lies within WPS010 VTC Collaboration Service as a service feature, and not within WPS008.)

Listed below the main ESOC Service features:

- Single Point of Contact (SPOC):
  Single point of contact between the service provider and the users for what concern services disruptions, services requests, or even for some categories of request for change (RFC). Notwithstanding the complex organization behind the Operations Centre Service delivery, it provides a point of communication to users and a point of coordination for several IT groups and processes. This feature is further eased by the establishment of a single telephone extension enabling Users across NATO to benefit from full range of the Agency's support capabilities via a single point of contact and gain extraordinary efficiency in terms of overall costs and Incidents / Requests resolution time.

- Request for Information (RFI):
The centralized Service function enables the possibility to request and receive information about service requests and their status, provide an interface for other activities such as customer change requests, maintenance contracts, SLM, service asset and configuration management, availability management, IT service continuity management and assist with general information, complaints or comments.
- Duty Control Officer (DCO) Team:
The ESOC Service enables the command and control node, making decisions in real-time regarding disposition and employment of NATO’s C4ISR assets, within the constraints provided by political, legal and contractual direction. The Duty Control Officer (DCO) Team supports the Service to execute this function by having an Officer on duty at all times, 24/7/365. DCO is also responsible to maintain the liaison with designated user representatives in order to provide situational awareness and de-conflict cross-customer operational priorities. Duty Control Officer Team play also an active role by implementing the proper levels and timescales in functional and hierarchical escalation of incidents, Major incidents, problems and customers’ complaints.
- Incidents Management:
ESOC Service provides the lifecycle management of IT incidents of all NCI Agency Services with the aim to restore as quickly as possible unexpectedly degraded or disrupted services to users and minimize impact to operations. Incidents may be recognized by technical staff, detected and reported by event monitoring tools, communications from users (usually via a telephone call to the service desk), or reported by third-party suppliers and partners. Operations Centre Service ensures that incident management activities support agreed service levels and objectives by prioritizing those activities based on actual operational need. Service assists Service Level Management (SLM) to define measurable responses to service disruptions and to review SLAs objectively enabling to determine the actions necessary as part of the service improvement plan (SIP), where required.
- Service Requests Management:
ESOC Service provides the lifecycle management of all Users’ generated service requests. Listed below the value this Service feature brings to Users:
    - Ability to provide quick and effective access to standard services that operations staff can use to improve their productivity;
    - Ability to effectively reduce the bureaucracy involved in requesting and receiving access to existing or new services, thus also reducing the cost of providing these services;
    - Ability to increase the level of control over requested services through a centralized fulfilment function. This in turn can help reduce the cost of support.
- Network Monitoring and Events Management:
ESOC Service manages Network and monitored IT infrastructure events throughout their lifecycle to include the coordination activities to detect events, make sense of them and determine the appropriate control, response and escalation actions. Listed below the indirect Service feature benefit:
    - Provides mechanisms for early detection of incidents. In many cases, it is possible for the incident to be detected and assigned to the appropriate group for action before any actual service outage occurs.

- Makes it possible for some types of automated activity to be monitored by exception – thus removing the need for expensive and resource-intensive real-time monitoring, while reducing downtime.
- Provides recommendations for automated operations, thus increasing efficiencies and allowing expensive human resources to be effectively used.
- Has a direct bearing on service delivery and customer satisfaction.

Service Flavours:

The Service is available as a single flavour.

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Minerva and Mission networks currently have their own local Service Desk that will survive as long as the special Network domain exist and/or the CSD can provide the same level of service.

Service prerequisites: None

Standard Service support levels: The ESOC Service is available 24/7.

Available hours	**First Call Resolution Target**	**Target Time to Pick Up**
24/7[1]	75%	• 75% ≤ 20s • 80% ≤ 30s • 85% ≤ 60s

[1] Outside the working hours, during the Weekends and SHAPE Holidays, the Operations Centre Service is available 24/7 with same quality targets assuming that the Customers' call volume and Services support demand is reduced. Any exceptions on Service demand outside the "SHAPE working hours" (ex: Exercise Support, Ministerial, etc.) as well as to Service Level Targets are subject to a Price Proposal (PP).

Service Cost / Price: The unit of measure for the Service is "Per Device", in accordance with the quantity of devices requested through WPS001, WPS006 and WPS016 (For WPS016, only Tablet and Smart Phone quantities). For price details please see the Service Rates Document.

WPS009 Unclassified Voice Collaboration Service

Service ID: WPS009

Service Name: Unclassified Voice Collaboration Service

Portfolio Group: Workplace Services

Service Description: The Voice Collaboration Service provides the ability to collaborate and communicate through audio with the telephony subscribers on NATO and National military unclassified networks, as well as commercial fixed and mobile telephony networks.

Value proposition: The Service allows voice communication between two or more parties from any location. This increases flexibility and saves cost, as no travel is required.

Service Features: The different device modalities (analogue phone, Voice over IP phone, Software Client, etc.) as well as service features are highly dependent of the specific location where the service is provided. Same applies for the various features and functions such as conferencing capabilities, hunt groups, voice mail, pickup-groups, call forwarding, etc.

With each instance of the service, either a static desk phone or a Software Client will be provided with an assigned telephone number, consisting of an internal 4-digit extension and a location-based prefix.

With the assigned telephone number, the user can place and receive calls to/from NDN, NCN and commercial networks. To be able to call from softphone a local national breakout connection to commercial networks is required

Service covers in-service support of end-to-end telephony services including the replacement of hardware and software in case of an incident. Default calling permissions (flat-rate contract) includes calls to all NATO subscribers, National Military networks and Europe (including US, Canada, Turkey) telephony networks. Other calling permissions can be provided but they are subject to customized configuration.

The procurement of software and hardware (including end-user devices) and lifecycle replacement is excluded from the service support cost (O&M) and must be procured separately.

Service Ordering and Request: The new service instances are requested by submiting a Customer Request Form (CRF).

After a service is initiated, the in-service support phase for the service is managed through annual Service Agreements with each customer.

The service fee for this service is charged to each Agency customer directly, meaning the service charges are not covered by the NATO central funding channels for NATO, therefore each customer requests/orders this service directly themselves.

For IT Incidents, Request for Information (RFI) and Service Requests (SR) regarding this service, the Operations Centre is the NCI Agency's Single Point of Contact (SPOC) for all eligible Customers and Users.

Service Flavours:

Available flavours are the following:

Voice Collaboration (Calling) Service: Provided as a telephone number and assigned to a Desk Phone or a Softphone (via Skype for business). The user can place and receive calls from/to the assigned telephone number.

Business-to-Business Federation (B2B)[1]**:** Provides NATO users the possibility to communicate through audio with external Voice networks such as Nations, Missions, Deployed CIS, NGO's.

Available on:

Static Desk Phone: NATO Voice Network. Highest content classification: UNCLASSIFIED

Softphone (Skype for Business): Available on NU and REACH networks. Highest content classification: UNCLASSIFIED

Service prerequisites:

INF001 LAN Service

WPS012 Workstream Collaboration Service (for Softphone only)

Standard Service support levels:

Service Availability[2] **Target:** 99.5%

Standardised time to deliver new service instance[3]: 3 working days (installation and configuration of new phone device)

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

Higher service availability and restoration targets can be negotiated and funded through the respective SLAs.

ACO/ACT Customers: Incident prioritisation and service restoration requirements are in accordance with the Aligned Baseline Incident Priority Assignment Table (ABIPAT) agreed in the SLAs. Service Request / Request Fulfilment prioritisation and service installation requirements are in accordance with implementation time targets agreed in SLAs.

[1] B2B is not applicable to common-funded Customers

[2] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

[3] Provided the underlying infrastructure is ready and devices are on site

Other Customers. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency SLAs and SSPs with respective customers.

Service Reporting:

ACO/ACT Customers: The standardised service reporting is provided as a deliverable of this service. ACO standardised reporting templates are listed in the SLA Annex 18 and managed by ACO KPI/KQI WG.

Quarterly Reports:

Service availability and service performance reports at Service Access Point (SAP) (via incidents)

Incident management report base on ITSM tickets and trend analysis

Change management and ASI report based on ITSM tickets

Phone billing service for the period (optional, upon request)

Asset and Configuration Management report

Additional service reporting requirements can be requested through the respective SLAs it may be subject to additional service fees.

Available NCI Academy Training not covered by service cost:

A0095	NATO Voice over IP Foundation
A0097	NATO Call Manager & Voice over Secure IP (VoSIP)
A0101	NATO C4ISR Orientation for Officers and NCO's
A0932	DCIS CES Voice Technician

Please note that this training is not funded through the service rate and it is added in the catalogue to familiarize the service users community with the available courses as part of the agency academy courses offerings.

Service Cost / Price:

The unit of measure for the Voice Collaboration (Calling) Service is per the telephone number assigned. The unit for the Business-to-Business Federation (B2B) service is per instance implemented.

Please see Service Rates document for standard rates applicable to the service.

WPS010 Video (VTC) Collaboration Service

Service ID: WPS010

Service Name: Video (VTC) Collaboration Service

Portfolio Group: Workplace Services

Service Description: The Video (VTC) Collaboration Service provides users the ability to collaborate and communicate through video and audio. It allows users from different geographical location to have face-to-face like collaboration as well as it supports multi-user, multi-location collaboration.

Value Proposition: The Service allows individuals and groups to interact easily, which enables a more flexible and efficient exercise of the Command and Control with significant savings in travel time and cost.

Service Features: The Service features include scheduling, VIP monitoring, conferencing, recording, playback and streaming, and connectivity of third parties.

Service Flavours:

WPS010-1 VTC Soft Client: provides users with an application (Polycom RealPresence Desktop) installed on the managed/qualified device. The flavour requires a camera and a microphone (in-built or as addition).

This is a best-effort service and HD quality is not guaranteed due to infrastructure limitations. Please also note that the infrastructure has a limitation for 500 concurrent calls.

WPS010-2 VTC System Only: consists of a VTC CODEC, which is integrated in a non-NATO Studio Wide VTC Room (a conference room with audio/video assets which belong to the local site and is therefore not part of the VTC Service).

WPS010-3 Desktop Dedicated Terminal: provides users with a dedicated VTC terminal (Polycom) connected to the network, which can be either:

- Desktop VTC Terminal, or
- Huddle/small room based system.

Conference room VTC: integrates with Conference room setups that become VTC enabled – it's provided with a camera and microphone and can be integrated with Conference room projection and presentation devices. The flavour has a range of room systems depending on their size, number supported participants, and the need for mobility, as follows:

- Roll About VTC system:
  - **WPS010-4 VTC Room - Roll About SDS (Single Domain);**
  - **WPS010-5 VTC Room - Roll About DDS (Dual Domain);**
- **WPS010-6 15-man room VTC system (dual domain system);**
- **WPS010-7 25-man room VTC system (dual domain system);**
- **WPS010-8 50-man room VTC system (dual domain system);**

- **WPS010-9 175-man room VTC system (dual domain system).**

WPS010-10 Immersive Telepresence Meeting (ITP) Room VTC : This service flavour uses enhanced **c**onference room technologies and provides the illusion of an in person meeting through the use of multiple screens in an `across the table` setup. Available only as single domain system.

WPS010-11 VTC B2B (Business to Business) Connection: provides a possibility to communicate through audio and video between NATO users and external VTC networks such as Nations, Missions, Deployed CIS, NGO's and GO's.

Available on:

NATO Unclassified (including public access)
NATO Restricted
NATO Secret
NATO Partner Network (For NNHQ)

Service Prerequisites:

WPS001 Managed Device Service (or qualified connected device) for VTC Soft Client Flavour.

Standard Service Support Levels:

Service Availability Target: 99.0% (exception: Soft Client flavour)

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A0244	NATO HD VTC Facilitator

Please note that this training is not funded through the service rate and it is added in the catalogue to familiarize the service users community with the available courses as part of the agency academy courses offerings.

Service Cost / Price: The unit of measure for the Service is Per Client Device, except for the VTC B2B flavour, where the unit of measure is Per VTC B2B Package. A VTC B2B Package includes up to 300 calls per year, limited to up to 5 simultaneous calls.

Please see Service Delivery Lifecycle Stages section for the lifecycle stages of a service along with the corresponding deliverables and the service rates applicable in each stage.

Please see Service Rates document for standard rates applicable to the service.

In special cases there are discounts offered:

	Case	Discount
1	The customer has its own local support contract for equipment maintenance	10%
2	The customer provides the L1 support	20%
3	Combination of 1 and 2	30%

Service Reporting:

ACO/ACT Customers: The standardised service reporting is provided as a deliverable of this service. ACO standardised reporting templates are listed in the SLA Annex 18 and managed by ACO KPI/KQI WG.

Quarterly Reports:
Service availability and service performance reports at Service Access Point (SAP) (via incidents)

Incident management report base on ITSM tickets and trend analysis

Change management and ASI report based on ITSM tickets

Asset and Configuration Management report

Additional service reporting requirements can be requested through the respective SLAs it may be subject to additional service fees.

WPS011 IP Television (IPTV) Service

Service ID: WPS011

Service Name: IP Television (IPTV)

Portfolio Group: Workplace Services

Service Description: IP Television Service provides the user with commercial cable television service as well as NATO specific channels. This service provides numerous channels, primarily focused on news and informational events, and offered in a variety of languages used in NATO.

Value Proposition: The IP Television Service offers the user an ability to leverage a fully managed and operated contractor service inside the New NATO Headquarters. This allows the user to keep up to date with news events. In addition to commercial news, the user can also view NATO channels which provide NATO news as well as can provide streamed videos of HQ briefings. This aids operational efficiency and effectiveness and supports situational awareness throughout the headquarters.

Service Features: The IP Television Service includes a fully managed and operated commercial capability augmented with NATO information. IP Television can be a full service providing the television, trolley and channels or as small as offering the channels and a connection SetTopBox (STB).

Business users can access three of the main news channels on their NATO managed mobile device.

Nations and staff can request additional channels that offer specific programming or national specific content. These channels can be ordered separately and the price is based on the requested licensing.

Service Flavours:

IP Television – This service supports the office environment. The 55” television is mounted on a trolley and connected to the floor box plug in a specific office or meeting room

Soft client – This service flavour allows the users to access the IPTV channels from their devices, provided through the managed device services.

Available on:

IPTV Flavour – Public networkSoft client flavour – NATO Restricted and NATO Unclassified

Service Prerequisites:

WPS001 Managed Device Service (for Soft client Service flavour)

Standard Service Support Levels:

Service Availability Target: 99%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.
N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is Per Device.

Please see Service Delivery Lifecycle Stages section for more information about the general overview of the type of deliverables involved in each stage and the scope of corresponding service rate.

Please see Service Rates document for standard rates applicable to the service.

#	Channel Name	#	Channel Name
1	La Une	23	CNBC-E
2	La deux	24	Sky news
3	La trois	25	Channel 5
4	France24	26	ITV 1
5	TV5Monde	27	ITV 2
6	BBC World	28	ITV 4
7	MTV	29	BBC News
8	CNN	30	ITV 3
9	Euronews	31	RTP-International
10	Nederland 1	32	RAI News24
11	Nederland 2	33	TVR International
12	Nederland 3	34	ARD
13	BBC1	35	TV-8
14	BBC2	36	ATV
15	National Geographic Channel HD	37	TRT 1
16	RAI 1	38	TRT 2 (Haber)
17	RAI 2	39	TRT Turk
18	RAI 3	40	CNN Turk
19	Animal Planet	41	Haber Turk
20	Aljazeera	42	TGRT
21	Discovery Channel	43	TA3
22	Eurosport	44	PRO TV International

WPS012 Workstream Collaboration Service

Service ID: WPS012

Service Name: Workstream Collaboration Service

Portfolio Group: Workplace Services

Service Description: The Worksteam Collaboration Service provides a persistent, shared conversational workspace that helps NATO staff initiate, organize and complete their daily work. Solutions offered to NATO staff members integrate direct and group messages, alerts, notifications, activity streams, and real-time audio and video into searchable groups or channels.

Value Proposition: The service supports both ad-hoc collaboration (Instant Messaging, chat, real-time audio/video, informal e-mail, etc.) as well as the more team-focused collaboration needs (search, group community collaboration, etc.).

Service Features: WPS012 (Workstream Collaboration Service) is an amalgamation of former WPS004 (E-mail Service) and WPS005 (Instant Messaging and Collaboration Service) and covers the informal and unstructured aspects of collaboration within the future NATO Digital Workplace.

Standard Microsoft Exchange Mailbox is accessible through a thick mail client (MS Outlook) or through the web-based client (OWA). Mailboxes are available to support individuals or groups; e.g. personal mailbox, functional mailbox or group mailbox. The standard mailbox size is 10GB.

Standard Instant Messaging is based on Microsoft Skype for Business platform and provides enhanced presence support (i.e., user online, offline, busy), single or multi-user conversation, audio and video call, telephony integration, and desktop sharing; however, some features might not be available on selected domains due to security restrictions.

For the more formal, i.e. consultation, aspects of collaboration please refer to WPS010 (Video (VTC) Collaboration Service).

*Note: Each instance of the Service will be counted separately (i.e. if the same user is using two different instances of WPS012 on two different networks, the user will be counted twice

Service Ordering and Request: The new service instances are requested and created by submitting standardised service request (work order) through the ITSM toolset; for customers there is no specific service initiation cost associated with Workstream Colaboration Service. 1

After a service is initiated, the in-service support phase for the service is managed through annual Service Agreements with each customer.

[1] Non-common funded customers via a Customer Request Form (CRF)

The service fee for this service is charged to each Agency customer directly, meaning the service charges are not covered by the NATO central funding channels for NATO, therefore each customer requests/orders this service directly themselves.

For IT Incidents, Request for Information (RFI) and Service Requests (SR) regarding this service, the Operations Centre is the NCI Agency's Single Point of Contact (SPOC) for all eligible Customers and Users.

Service Flavours: The service is available as a single flavour.

- Note: External customers can purchase WPS012EF (External Federation): This flavour when purchased enables the entity to federate with NATO e-mail or Skype for Business services on the available networks the service is provisioned at. It contains only the fees to configure and bring the service alive in terms of human resource and Microsoft consultancy. It does not include any hardware or license fees required by the federating entity. The service is per capability, either e-mail or Skype for Business. When both capabilities are federated, the fee is two times the service cost.

Available on*:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret
Other specialized NATO networks (e.g. NATO Partner network and alike)

*Note: The features and functionality available in each network can deviate due to security constraints and local security policies as determined by the relevant Security Accreditation Authority (SAA). Equally, the products used to provide the service can be different depending on the classification of the network in use.

Service Prerequisites:

WPS001 Managed Device Service (connected or stand-alone flavours)
WPS002 Enterprise Identity Access Management Service
WPS003 Enterprise User License Service (or equivalent Microsoft Enterprise User License procured through other channel)

Standard Service Support Levels:

Service Availability Target: 99.0%

Standardised time to deliver service: 1 working day (creation of new e-mail account)

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full priority resolution times and generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Reporting:

ACO/ACT Customers: The standardised service reporting is provided as a deliverable of this service. ACO standardised reporting templates are listed in the SLA Annex 18 and managed by ACO KPI/KQI WG.

Quarterly Reports:

Impact on service availability and service performance reports at Service Access Point (SAP) (via incidents)

Incident management report base on ITSM tickets and trend analysis

Change management and ASI report based on ITSM tickets

CIS Security and Cyber report

Asset and Configuration Management report

Additional service reporting requirements can be requested through the respective SLAs which are subject to NCIA's cost and feasibility assessment.

Service Cost / Price: The unit of measure for the Service is "per user instance". Since the Service is designed for the general use by all the users of each customer, the number of user instances will be assumed to be equal to the sum of the "NATO Peacetime Establishment (PE)" users plus the "NATO Non-Peacetime Establishment (NPE)" users for each network where the service is consumed.

Each instance of the Service will be counted separately (i.e. if the same user is using two different instances of the Service on two different networks, the user will be counted twice).

All exceptions to the service instance calculation method will be agreed between the Provider and the Customer and documented in the individual SLAs/SSPs accordingly.

WPS014 Secure Voice Service

Service ID: WPS014

Service Name: Secure Voice Service

Portfolio Group: Workplace Services

Service Description: The Secure Voice Service is a voice collaboration service that provides user with the ability to collaborate and communicate through audio and audio/video in a secure network environment. The Service enables communication to other Voice Secure Domains outside of NATO VoSIP network (e.g. BICES).

Value Proposition: The Service enables real-time secure communication between more parties. This dramatically increases the effectiveness of the Command and Control and provides additional flexibility and efficiency to it, by saving time and cos of usually required travel.

Service Features: Secure Calls, Secure Video Calls, Secure Conferencing Calls, Secure Video Conferencing Calls, Hunt Groups, Pick Up Groups, Call Forwarding, and Extension Mobility Service are provided on the available NATO security domains.

Service Flavours:

WPS014-1 Secure Voice Service - Desk phone (Voice): provides a static Voice over IP Desk Phone and a secure voice telephone number assigned.

WPS014-1 Secure Voice Service - Desk phone (Voice/Video): provides a static Voice over IP Desk Phone with additional video capability and a secure voice telephone number assigned.

WPS014-2 Secure Mobile phone (SECTRA)[1]: provides a mobile ability to collaborate and communicate through audio in a closed secure network environment. The device allows voice connections up to SECRET level and SMS up to RESTRICTED level.

WPS014-4 Business to Business Federation (B2B): provides NATO users the possibility to communicate through audio and video with external Voice networks such as Nations, Missions, Deployed CIS, NGO's and GO's.

Available on:

NATO Secret

Mission Secret

Service Prerequisites:

INF001 LAN Service

SEC011 Gateway Security Service (To Secure Domains outside NATO VoSIP Network)

[1] Hardware Connector to a Secure Mobile Phone Flavour (Tiger/S 7401 docking station connector) – can be provided when needed as part of the service rate without O&M extra charges, commands can buy the cable/connector through the CRF process whenever needed.

Standard Service Support Levels:

Service Availability[1] Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A0095	NATO Voice over IP Foundation
A0097	NATO Call Manager & Voice over Secure IP (VoSIP)

Service Cost / Price: The unit of measure for the Service is Per Device for all flavours except for **Voice Business to Business (B2B) flavour the unit of measure is per B2B connection**

Please see Service Rates document for standard rates applicable to the service.

Service Reporting:

ACO/ACT Customers: The standardised service reporting is provided as a deliverable of this service. ACO standardised reporting templates are listed in the SLA Annex 18 and managed by ACO KPI/KQI WG.

Quarterly Reports:

Service availability and service performance reports at Service Access Point (SAP) (via incidents).

Incident management report base on ITSM tickets and trend analysis.

Change management and ASI report based on ITSM tickets.

Asset and Configuration Management report.

Additional service reporting requirements can be requested through the respective SLAs it may be subject to additional service fees.

WPS015 Voice Loop Service

Service ID: WPS015

Service Name: Voice Loop Service

Portfolio Group: Workplace Services

Service Description: The Voice Loop Service provides the user with the ability to communicate with a group of users through audio.

Value Proposition: Voice Loop Service allows easy communication between more than one party (CAOC's and CRC's). This increases reliability, flexibility and response time to Static Air Defence Centre mission of Air and Controlling Policing over NATO North and South Region.

Service Features: The Service allows the user to participate in different Conferences (Voice Loops) established with different locations with the ability of IP Voice recording.

Voice Loop Conferences: Voice Loop provides the user the ability to participate in a permanent open conference with all the participants in a specific region.

Voice Recording: Allows IP Voice capture and preservation system, therefore constant recording of all Voice Loop voice content

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified

Service Prerequisites:

For IP Phone: INF001 LAN Service
For Networking: INF005 Infrastructure Integration Service
For Communication: INF014 Transmission Service

Standard Service Support Levels:

Service Availability Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A0095	NATO Voice over IP Foundation
A0097	NATO Call Manager & Voice over Secure IP (VoSIP)

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

WPS016 Enterprise Managed Mobility Service

Service ID: WPS016

Service Name: Enterprise Managed Mobility Service

Portfolio Group: Workplace Services

Service Description: The Enterprise Managed Mobility Service provides the users with various flavour of mobile solutions ranging from a basic cellular subscription to fully managed mobility solutions enabling users to connect to NATO Unclassified or NATO Restricted networks. The more advanced Enterprise Mobility flavour provides the capability to connect a managed Apple iOS device (Smartphone or Tablet) to NATO Unclassified or NATO Restricted services such as e-mail and other enterprise business applications.

Value proposition: The Service offers a single customer experience when accessing NATO networks from a range of managed Apple iOS smartphone and tablet devices. The service allows for better availability of staff and fast reaction to critical action items while being distant from the office.

The procurement of software and hardware (including end-user devices) and lifecycle replacement is excluded by the service cost and must be paid separately.

Service Features: The service provides mobile users with the capability to access Enterprise Applications and mobile apps, in line with NATO security requirements. In detail, the Service features are:

- Managed device in accordance with the NATO security guidelines;
- Mobile subscription, cellular provider expense management, and data cost management;
- Productivity mobile apps (e.g. mail app, collaboration apps, web browser).

Service Flavors (for customer ordering)

WPS016-A Smartphone/Tablet (iOS device only)
Covers the Life-Cycle management of the Smartphone/Tablet provided by the NCI Agency
(Dependency: WPS008 Enterprise Services Operations Centre (ESOC) Service)

WPS016-B1 Cellular Subscription (Profile Plan 1 - Basic) (*note)
Unlimited SMS/Calls in EU+[1]
Unlimited SMS/Calls in USA (if user is based in the USA only)

WPS016-B2 Cellular Subscription (Profile Plan 2 - Standard) (*note)
Unlimited SMS/Calls in EU+
10GB internet in EU+

[1] **EU+** includes the following countries: EU 28 + UK, Aland (Finland), French Guyana, Iceland, Liechtenstein, Martinique, Norway, Reunion, San Marino, Saint Martin, Saint Barthelme, Guadeloupe, Gibraltar (UK), Vatican

Unlimited SMS/Calls in USA (if the User is based in the USA only)
10GB internet in USA (if the User is based in the USA only)

WPS016-B3 Cellular Subscription (Profile Plan 3 - Traveller) (*note)
Unlimited SMS/Calls in EU+
10GB internet in EU+
Unlimited SMS/Calls in USA (if the User is based in the USA only)
10GB internet in USA (if the User is based in the USA only)
3GB in Extended Roaming Countries*[1]

WPS016-B4 Cellular Subscription (Profile Plan 4 - Traveller Unlimited) (*note)
Unlimited SMS/Calls in EU+
Unlimited Data in EU+
Unlimited SMS/Calls in USA (if the User is based in the USA only)
Unlimited internet in USA (if the User is based in the USA only)
5GB in Extended Roaming Countries

WPS016-B5 Cellular Subscription (Profile Plan 5 - Data Plan Hotspot) (*note)
Unlimited GB Data in EU+
Unlimited GB Data in USA (if the User is based in the USA only)

WPS016-C Enterprise Managed Mobility Service (NU/NR)
Provides the capability for remote access to business collaboration tools via Apple iOS Smartphone/Tablet. It also provides remote connectivity for WPS001-C Portable (Laptop/Tablet) Device in case it has WiFi or cellular capabilities enabled.
(Dependency WPS016-A or WPS001-C)

***note: The subscription cost is location/country specific and only indicated as an average for SLA/SSP planning purpose. NCI Agency will conduct a competition for a NATO-wide Global Mobile Telephony contract has been put in place early 2023.**

Note 1: Due to supply chain security and other important security considerations, any smartphone and/or table connecting to a NCI Agency supported CIS shall have both the actual device (WPS016-A) *and* its cellular subscription, i.e. SIM Cards (WPS016-Bx), provided by the NCI Agency.

Note 2: Tablets can be provided with an optional SIM card slot installed which can be used for gaining access to the Internet. If the SIM card slot is utilized in tablets that connects remotely to a NCI Agency supported CIS, the cellular subscription must be provided via WPS016-B5 service flavour.

*[1] **Extended Roaming Countries includes:** Albania, Australia, Bosnia and Herzegovina, Brazil, Canada, Cape Verde, China, Egypt, Guernsey (Bailiwick of), Hong Kong, India, Indonesia, Israel, Japan, Jersey Island, North Macedonia, Man (Isle of), Mexico, Montenegro, Morocco, Republic of Türkiye, Russian Federation, Serbia, Singapore, South Africa, Switzerland, Thailand, Tunisia, Ukraine and United States of America.

Provision of cellular subscriptions for legacy devices or Phones not provided by the NCI Agency is optional through WPS016-B1 or WPS016-B2 service flavour only.

Note 3: Customers who selects only the WPS016-A service flavour, i.e. the device only without a cellular subscription, will have the device considered as a SIM Less device. Customers will be able to use their own cellular subscriptions while still have a supported smartphone/device.

If a customer wants to utilize their own cellular subscription together with the WPS016-C Enterprise Managed Device Mobility (NU/NR) service flavour, the NCI Agency will need to review the contractual and legal agreements of the customer's cellular subscription. This is mandatory to ensure the required contractual and legal frameworks are in place for secure and reliable connectivity to a NCI Agency supported CIS. The cost for the review will be charged to the customer on a cost reimbursable basis.

Service options (additional charges apply):

- Mobile Secure Communication on smartphones – provides secure voice solutions on smartphones, up to NATO Restricted level by using commercial solution based on SecuSUITE.
- Other specific applications*:* special mobile apps such as custom developed app for orientation in the NATO HQ building.

Available on:

Standalone (see note 3 above)

NCI Agency supported CIS on low side (NU/NR)

Service Prerequisites:

WPS016-A:

- WPS008 Enterprise Service Operations Centre (ESOC) service

WPS016-C:

- Applicable user account (WPS002 Enterprise Identity Access Management Service) on the NCI Agency supported CIS that connectivity is required to.

Standard Service Support Levels:

General service availability target is 99.0% with Priority Resolution Times and Generic Service Priority Assignment Matrix in accordance with the NCI Agency standardised Service Level Agreements in force.

- Standard Support: 08:30 - 17:00 (included in standard service rate)
- VIP Support: 06:00 - 22:00 (service rate available upon request)
- VVIP Support: 00:00 - 23:59 (i.e. 24/7 support) (service rate available upon request)

For ACO/ACT customers: Incident prioritisation and service restoration requirements are in accordance with the Aligned Baseline Incident Priority Assignment Table (ABIPAT) agreed in the SLAs. Service Request / Request Fulfilment prioritisation and service installation requirements are in accordance with implementation time targets agreed in SLAs.

Service Cost/Price:

The unit of measure of the first flavour (WPS016-A) Smartphone/Tablet (iOS device only) is per device.

The service rate used for service costing of cellular subscriptions, (i.e. WPS016-B1 to B5), is per SIM Card.

The exact service rate varying from country to country. For 2024 *budgetary purposes* the following annual service rates are recommended to be used:

***Please note that cellular subscriptions will be charged as per actual usage and above service cost is solely for budgetary and planning purposes. Customers will be provided with monthly usage reports enabling close cost control on the actual utilization.**

This page is left blank intentionally

Infrastructure Services

This page is left blank intentionally

INF001 Local Area Network (LAN) Service

Service ID: INF001

Service Name: LAN Service

Portfolio Group: Infrastructure Service

Service Description: The LAN service provides users with local network connectivity. The LAN service is crucial to enable collaboration and communication. The LAN service is provided as a cabled infrastructure for all networks and as a wireless infrastructure for accessing only the unclassified and restricted networks.

Value Proposition: The LAN Service is a vital component enabling all local users to connect to the wider network. It is the key enabler for accessing all NATO customer facing services such as Voice and Video, as well as Internet, and enabling services such as security and management. The Service allows all entitled users to access shared NATO services and data across the NATO Enterprise.

Wi-Fi connections provide additional flexibility, allowing users to connect to the network from anywhere within the relevant Wi-Fi footprint, preventing users from being 'tied' to their desks.

Service Features: LAN Service is available on the NATO Security domains in wired and, in selected locations, as Wireless (Wi-Fi) configurations. The LAN Service will be capacity sized to support the number of connected devices and Users. This is with the understanding that all equipment is located within the same building and that the cabling system is available. The service does not cover the cabling through the building walls, as this is considered part of the building infrastructure.

Service Flavours: The LAN Service is available in the following flavours:

Wired – This service flavour provides a physical connection to terminate and connect devices to one of the NATO networks.

By utilising NCIA deployed LAN Service, users are able to operate on all wired NATO networks including, but not limited to:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret (when invoked)

Wireless - This service flavour provides the ability to connect a specific client device to a network wirelessly.

By utilising NCIA deployed LAN Service, users are able to operate on all wireless NATO networks including:

NATO Unclassified

NATO Restricted

Available on:

NATO Unclassified
NATO Restricted
NATO Secret – only wired
Mission Secret (when invoked) – only wired

Service Prerequisites:

INF002 NGCS PoP Service

Standard Service Support Levels:

	Availability Target	**Service Restoration Period**
During Support hours	99.9 %	1 hour
Outside Support hours	99.5 %	4 hours

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

While this provides a standard availability target for the service, regional support arrangements and therefore the availability targets may vary and should be agreed during the SLA discussions.

Service Cost / Price: The unit of measure for the Service is Per Port, with 24 ports being the minimum orderable quantity. The number of ports required for a customer is in accordance with the quantity of devices requested through WPS001, WPS006 and WPS016 (For WPS016, only Tablet and Smart Phone quantities) multiplied by 2.

Please see Service Delivery Lifecycle Stages section for more information about the general overview of the type of deliverables involved in each stage and the scope of corresponding service rate. Please see Service Rates document for standard rates applicable to the service.

INF002 NATO General Purpose Communication System (NGCS) Point of Presence (PoP) Service

Service ID: INF002

Service Name: NATO General Purpose Communication System (NGCS) Point of Presence (PoP) Service

Portfolio Group: Infrastructure Services

Service Description: The NGCS PoP Service primarily provides the infrastructure at points between communicating entities, where a connection is required. The NATO Network POP Service is defined as the provision of the infrastructure assets, capacity provisioning, and cyber security management elements that enable the user to establish any-to-any connectivity at supported sites and between connected networks. It has a dependency on INF014, which provides the connection between sites. At each security domain classification, this service is a direct enabler of other customer facing services like: INF001, INF035, as well as 3rd party customers serviced via Point to Point EVCs or PCN type interfaces.

Value Proposition: The Service is an integral component in enabling users to connect and collaborate between each other in support of the majority of NATO business activities and processes.

Service Features: The Service is available across all NATO Security Domains. It features the WAN Infrastructure Assets (Protected Core Access equipment in line with the valid Technical Architecture) and Cyber Security Management (layered security present at connectivity access points).

NGCS Service Flavours: The exact specification of each service flavour may vary subject to equipment and suppliers but can be described as follows:

- **INF002 – NLI PoP:** this flavour provides the termination of medium bandwidth transmission services with links from 100 Mbit/s up to 10 Gbit/s. PoP flavour is required to support user communities larger than 100. These PoPs are generally Common Funded and include a Network Edge Device (NED) e.g. HQ SHAPE. This service flavour is to be made available only for the duration of migration of services between the legacy NGCS POP service and the NCI service flavour described below.

- **INF002P - Pico PoP:** this flavour provides the termination of medium bandwidth transmission services with links up to 100 Mbit/s. Pico PoP flavour supports user communities up to 100 users. PicoPoPs are generally customer (SSP) funded and include a Customer Edge Device (CED) e.g. NFIUs. They also provide dedicated or shared services to support NNCCRS.

    - **INF002A - Pico PoP:** this flavour is modelled on INF002P above but follows a different funding model (cost reimbursable) and specifically supports AMDC2 services e.g. SRAP and ACCS.

- **INF002L - Legacy PoP (Remote extension)**: this flavour provides the termination of small bandwidth transmission services (less than 100Mbit/s links). Remote extension services are also required to support up to 100 users. Considered as a legacy connection for existing services that do not meet the NGCS target architecture requirements; it is no longer offered as a new service. It does not include a NED or CED. This service flavour is marked to be discontinued, with service delivery being migrated to the INF002 – NNG service flavour, in line with AFS concepts.

NGCS Service Flavour Enhancements: NGCS PoPs may be extended or enhanced with the following:

- **INF002N - NNG - NATO to Nation Gateway (NNG):** The NNG is an agreed hand over point between NATO and a Nation to allow information exchange for AIS (static) services. NATO is responsible to deliver the services to that point, whereas the Nation is responsible to provide connectivity and services from the NNG to the required location within the Nation. The NNG can be used for NS (future NR) and offers the option to include NS V2 services (SBC required). Additional security (i.e. firewalls on both sides) is required.
- **INF002NP - Network Interconnection Point (NIP):** A NIP is an agreed hand over take over point (Federated Mission Network compliant) between NATO and a Nation to allow information exchange for NRF, Exercises and Missions (this includes ships). NATO is responsible to deliver the services to that point, whereas the Nation is responsible to provide connectivity and services from the NIP to the required location within the Nation. The NIP can be used for (NRF) NU, (NRF) NR and (NRF) NS and offers the option to include V2 services (SBC required).
- **INF002LV - Local V2 Aggregation Router (LVAR):** An LVAR is deployed to enable delegated NMRs at the highest level of national command (e.g. CHOD / MOD) to access Secure Voice services. LVAR devices will be located within national NS infrastructures und national IT management. IPSEC tunnels will be created to connect to the NGCS. Nations are responsible for Level 1 support with Level 2 and 3 support from NCIA at best effort due to the services dependence on National Defence Network infrastructure.

NCI Service Flavours: The exact specification of this service is still under development but is likely to include:

- **NCI Nodes** – Core 40G, Enhanced 40G, Standard 40G and 5G.
- This flavour provides the latest service evolution for the POP service, and is a direct replacement for INF002 NLI, in regards to termination capabilities of medium bandwidth transmission services with links from 100 Mbit/s up to 40 Gbit/s. These PoPs are generally Common Funded and include multiple subsystems for Protected Core Access (PCA), Coloured Cloud Access (CCA) of multiple sercurity domains: NU, NS,NR as wel las Multi Media Access (MMA) for NU voice and video services.

Delivering capabilities on:

NATO Secret
NATO Restricted
NATO Unclassified

Service Prerequisites:

INF014 Enterprise Transmission Services (and NDNs for LVAR)

Standard Service Support Levels:

Service Availability Target (SAT): 99.5% and must below INF014 SAT.

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Availability for the NGCS POP Service is determined annually and is dependent upon enabling services and regional support arrangements. Availability target provided above is for 24/7 service, where the service option only in support hours will provide lower availability, to be agreed with the customer on the SLAs.

Service Cost / Price: The unit of measure for the service is per PoP.

Please see Service Delivery Lifecycle Stages section for more information about the general overview of the type of deliverables involved in each stage and the scope of corresponding service rate.

For the price details, see the Service Rate document.

INF003 Enterprise Internet Access Service

Service ID: INF003

Service Name: Internet Access Service

Portfolio Group: Infrastructure Services

Service Description: Enterprise Internet Access Service comprises of the provision and supply of secure web browsing connectivity to the internet, mail relay and mail security sanitation. Additionally this service supports collaboration and interoperability amongst any dependent NATO resources.

Value proposition: Enterprise Internet Access Service offers the user the access to the internet, enabling the user to conduct open source intelligence gathering, administration, welfare and many other activities to support their business needs.

Service Features:

- Downstream bit rates
- Upstream bit rates
- Monitoring from our Network Operations Centre
- High-speed access
- Secure access
- Corporate Web Proxying
- Corporate Internet DNS Service

Service Flavours: The service is available in the following flavours:

Standard Internet Access: is the standard internet provided across the enterprise based on the following principles:

- Access is controlled based on appropriate site categorisation, blocked for unappropriated site categories (Porn, Gambling, Storage on line, Etc.)
- Traffic of any kind is subject to inspection including SSL decryption as appropriate (exclusion for Banking, Health and Governmental institution)
- Exception to the above are organised by means of policy on user request approved by the local SSA

Anonymized Internet Access: is an internet access organised in a way that browsing result sourced from IP addresses are not attributable to NATO. Anonymisation is a data processing technique that removes or modifies personally identifiable information; it results in anonymised data that cannot be associated with any one individual or organisation (NATO in this case).

Available on:

NATO Unclassified
NATO Restricted

Service prerequisites:

WPS001 Managed Device Service

Standard Service support levels:

	Availability Target	Restoration Period
In support hours	**99.9 %**	**1 hour**
Out of support hours	**99.5 %**	**4 hours**

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is shown in the table above.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the service is 1, meaning that the cost/price of the service is calculated on the enterprise total cost basis.

Service Reporting:

ACO/ACT Customers: The standardised service reporting is provided as a deliverable of this service. ACO standardised reporting templates are listed in the SLA Annex 18 and managed by ACO KPI/KQI WG.

Quarterly Reports:

Impact on service availability and service performance reports at Service Access Point (SAP) (via incidents)

Incident management report base on ITSM tickets and trend analysis

Change management and ASI report based on ITSM tickets

CIS Security and Cyber report

Asset and Configuration Management reports

Additional service reporting requirements can be requested through the respective SLAs which are subject to NCIA’s cost and feasibility assessment.

INF004 Infrastructure Virtualization Service

Service ID: INF004

Service Name: Infrastructure Virtualization Service

Portfolio Group: Infrastructure Services

Service Description: The Infrastructure Virtualization Service is a flexible, scalable and redundant Infrastructure as a Service (IaaS) offering. It provides computing capabilities to provision and maintain virtual machines (VMs) in order to host databases, application and other services running on top of the operating systems to meet Customer's specific requirements.

Value Proposition: The Infrastructure Virtualization Service provides value to customers and other (customer facing) services by providing more control over scalability, better security of on-premises and private cloud compute devices. The service designed to be fully redundant and configured for automatic failover for compute resources in order to minimize downtime. This service is delivered mainly from central datacenters in multiple geographies. The service also offers the user with lower Total Cost of Ownership (TCO) of the virtualization infrastructure hosting as it is provided through a Shared Infrastructure model

Service Features: The Infrastructure Virtualization Service offers the user the following:

- Based on proven, best-in-class enterprise hardware and software
- Enterprise compute hardware and software procurement
- VMware Hypervisor administration including hypervisor level security hardening per NATO NOS standards, hypervisor and firmware upgrades and hypervisor patching
- Resource pool architecture, consisting of vCPU, vMemory, and shared SAN or software-defined storage
- Generally configured for high availability and dynamic resource allocation
- Flexibility to modify resource pools generally without VM downtime
- Dynamic scalability of resources to meet evolving requirements
- Guest Operating System for quick provisioning:
    - Windows Server (versions in A2SL only)
    - RedHat (RHEL) Linux (versions in A2SL only)
    - Oracle Linux (versions in A2SL only)
- Guest Operating System upgrades and patching:
    - Deploying Microsoft Security Patches to Windows Server virtual machines
    - Deploying RHEL / OEL OS Security patches to RHEL / OEL virtual machines
    - Deploying Emergency Patches / Battle Short to virtual machines
    - Patch Installation Types:
        - *Auto-patching* : Applied to VMs automatically during maintenance windows scheduled period without any specific databases and applications

  - *Manual patching*: The INF004 deploys and makes guest operating system patches available only. Application owners for VMs with specific database and applications install available patches themselves.

Note: Infrastructure Virtualization Service provide 'Virtualization' services on different data center levels in NCIA; Data Centers (DC), Enhanced Nodes (EN), Standard Nodes (SN), and Remote Nodes (RN) which depends on geographic location, network classification and capacity requirements. Not all features mentioned above are available in the four data center levels so during the requirements gathering the agency and customers shall mutually agree on the required features and hence the datacenter level is selected.

Service Flavours:

The Service is available as a single flavour but exceptionally for 2025 additional two flavours are included to reflect the implementation of ITM RC1. In the following years these two flavours will be removed and their cost will be redistributed into the relevant services.

Optional load balancing of infrastructure hosting to ensure availability for:

- Web sites
- SharePoint
- ADFS
- Exchange SMTP

INF004-2 SMC Discovery and TrueSight

BMC Discovery provides automated discovery and relationship mapping of network components, software, and related attributes. This information is directly loaded into the Remedy ITSM CMDB. BMC Truesight Provides the advanced monitoring and alerting functionality with event impact implications against service models.

INF004-3 Packaging

Covers the creation and initiation of packaging, dissemination and provisioning services, the packaging of applications for use on the VDI end user devices (EUDs), followed by the migration process of applications and data onto the new ITM ON. From a user perspective the execution of this work package will be seamless with minimum, if no, impact on service availability.

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret
Public Internet Access (PIA) Gateway

Service Prerequisites:

- INF001 LAN Service

- INF005 Infrastructure Integration Service
- INF007 Infrastructure Storage Service

Service lifecycle for Virtualization devices:

The criteria for obsolesce for devices is defined by '*NCIA's 10 year Lifecycle Plan*'. According to this plan, life expectancy for compute and HCI devices (called servers) is **'7'** Years unless the device is defined by the following criteria in order of urgency:

a. End of Service (EOS) devices
b. Failed of failing devices
c. Reported Missed SLAs as a result of failing devices
d. End of Life (EOL) devices

Standard Service Support Levels:

Service Availability Target: 99%

Built-in High Availability provides uniform failover protection against hardware and operating system outages within the virtualized IT environment offered by this service. High availability allows:

- Monitor VMware vSphere compute devices to detect hardware and system failures
- Restart virtual machines on other compute devices in the cluster without manual intervention when a server outage is detected
- Reduce application downtime by automatically restarting virtual machines upon detection of an operating system failure

N.B. Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A0311	NATO Data Centre Virtualization
A3024	Deploying VMware vSphere

Service Reporting:

Incident management report base on ITSM tickets and trend analysis

Change management and ASI report based on ITSM tickets

Additional service reporting requirements can be requested through the respective SLAs which are subject to NCIA's cost and feasibility assessment.

Service Cost / Price:

The unit of measure is infrastructure unit (composed of Infrastructure Virtualization, Infrastructure Storage, Infrastructure Backup and Infrastructure Integration Services). The rate included in the service rate is for an average sized infrastructure unit (4 vCPU, 20GB vMemory and 850GB vStorage).

INF005 Infrastructure Integration Service

Service ID: INF005

Service Name: Infrastructure Integration Service

Portfolio Group: Infrastructure Services

Service Description: The Infrastructure Integration Service provides the underlying infrastructure network services that are required to have a working IT environment. It ensures the availability and capacity of the Data Centres at several locations. It ensures the availability and capacity of the Data Centres at several locations. As a part of IaaS (Infrastructure as a Service) INF005 builds the basement for the centralized IT Infrastructure and create the hardware level for other centralized services. The fields of activity of Infrastructure Integration Service are Space, Cooling and Power inside the centralized NCIA IT Infrastructure. Also Network Time Protocol (NTP) is part of the service flavour provided by Infrastructure Integration Service. INF005 is a non-customer-facing service and is a prerequisite for Infrastructure Virtualization Service (INF004) and Storage Service (INF007) and Backup Service (INF016).

Value Proposition: The Infrastructure Integration Service is essential for a proper functioning IT environment. We plan, implement and manage the centralized IT environment within the NCIA IT Infrastructure.

Service Features:

- **Space:**
  - Physical Security
  - Classifications Security
  - Space Optimization
  - Space Utilization
  - Sustainability
  - Integration (Rack and Stack)
  - Migration
  - Cabling

- **Power:**
  - Distribution / Modernization
  - Redundancy
  - Control and Monitoring
  - Assessment

- **Cooling:**
  - Air Distribution
  - Efficiency Assessment
  - Control and Monitoring
  - Assessment

Service Flavours: The Service is available as a single flavour.

Available on: NATO Secret
Mission Secret
NATO Restricted
NATO Unclassified

Service Prerequisites: None

Standard Service Support Levels:

	Availability Target	Service Restoration Period
During Support hours	99.9 %	1 hour
Outside Support hours	99.5 %	4 hours

N.B. Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The service rate for this service is included under the service rate of INF004 Infrastructure Virtualization Service. No separate charges apply for this service specifically.

The unit of measure for INF004 is infrastructure unit (composed of Infrastructure Virtualization, Infrastructure Storage , Infrastructure Backup and Infrastructure Integration Services). The rate included in the INF004 service rate is for an average sized infrastructure unit (4 vCPU, 20GB vMemory and 850GB vStorage).

INF006 NATO Enterprise Directory Service (NEDS)

Service ID: INF006

Service Name: NATO Enterprise Directory Service (NEDS)

Portfolio Group: Infrastructure Services

Service Description: NEDSprovides the capability to share trusted identity information between different systems and to Enterprise users. The information on identities (e.g. people, organizations, and devices) is retrieved from different, authoritative sources (e.g. APMS). NEDS covers the whole enterprise (including NATO HQ) and will become the standard way to exchange identity information across NATO. Information can be synchronised between different affiliate systems and automated workflows can be created, including provisioning and de-provisioning of User Accounts. NEDS service information can be made available through either the NEDS native interface or through customized interfaces such as Web Access, file based interface or SQL access.

Value Proposition: NEDS provides value to customers through the sharing of identity information across multiple identity stores, improving data quality and reducing the administrative burden for connected systems. This ensures a coherent set of identity data from authoritative sources, while increasing the security posture of the NATO Enterprise.

Service Features:

Identity Management – through shared information across multiple identity stores, improving data quality and reducing the administrative burden for connected systems. Information can be synchronised between different affiliates, and automated workflows can be created, including provisioning and de-provisioning of User Accounts. This increases the security posture of the NATO Enterprise, while ensuring a coherent set of identity data from authoritative sources.

Data sources/consumers can make use of the NEDS native interface for retrieving or updating identity information using LDAP(S). Otherwise tailored interfaces can be developed based on for instance SQL or file based connectivity.

Currently Affiliated Systems:

- **Automated Personnel Management System (APMS)** - provides a manpower and personnel database for all users at every level within the NATO Command Structure (Bi-SC).
- **Bi-SC AIS Active Directory** – provides existing NS accounts and receives NEDS automatically created accounts for new NATO Staff users (originating from APMS) and updated existing NS accounts when APMS information changes for a NATO Staff user.
- **NATO Network Control System (NNCS) Database** – provides Formal Military Messaging (ACP 127) information related to Address Indicator Groups (AIGs), Signal Message Addressee (SMAs) / Plain Language Addressee (PLAs) and Routing Indicators (RIs) as well as NATO Subject Indicator Codes (SICs).

The affiliate administrator (AA) (customer of the identity management feature) of a subscribing affiliate can choose from available authoritative attributes what he / she can receive. If the AA needs additional attributes currently not contained in NEDS than NEDS can connect to an additional authoritative affiliate (if identified and available) and the AA can subscribe to these new attributes.

White and Yellow pages - For an end-user, NEDS provides search and browse functions through a web browser to access information (e.g. name, telephone number, email-address, and room number). As the functionality of the application is increased, this interface will also provide additional features, such as access request submission/approval and self-service updates.

Access to Web Portal by NATO Staff users is provided using HTTPS.

Service Flavours: The Service is available as a single flavour, with the following options:

White and Yellow pages - This web application provides the capability to search and browse for published information on identities from affiliated systems. It is accessed through a standard web browser and available to all customer staff.

Identity Management: On the identity management side, the affiliate administrator (AA) (customer of the identity management feature) of a subscribing affiliate can choose from available authoritative attributes what he / she can receive. If the AA needs additional attributes currently not contained in NEDS than NEDS can connect to an additional authoritative affiliate (if identified and available) and the AA can subscribe to these new attributes.

Available on:

NATO Secret

In the future, instances of the service will also be available on the NATO RESTRICTED/NATO UNCLASSIFIED environment.

Service Prerequisites:

None

Standard Service Support Levels:

Service Availability Target: 99.0%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

INF007 Infrastructure Storage Service

Service ID: INF007

Service Name: Infrastructure Storage Service

Portfolio Group: Infrastructure Services

Service Description: The Infrastructure Storage Service is a flexible, scalable, efficient and secure Infrastructure as a Service (IaaS) offering to store virtual machines and file shares (only on conventional storage devices) running on NCIA's Enterprise on-prem and private cloud infrastructure.

The Infrastructure Storage Service is provided through three main different storage types: block, backup, and object in order to best meeting business requirements to host virtual machines (VMs); shared-file systems like CIFS or NFS; backup data; long-time retention backups on conventional storage devices. These storage devices in the scope of this service description are only limited with conventional storage devices (or purpose-built storage hardware) along with its custom-made operating systems.

None of end-user storage devices included internal and external hard drives, flash memory-like devices are provided by this service.

Value Proposition: Infrastructure Storage Service provides value to customers and other (customer facing) services by storing virtual machines, virtual machine backups on-premises and private cloud storages efficiently.

Service Features: The Infrastructure Storage Service is comprised of the following features:

- Enterprise-class , high performance, highly available, redundant conventional storage infrastructure with optional long-term retention storage if/when requested by the Customers.

- Provisioning Logical Unit Numbers (LUNs) for Infrastructure Virtualization Service (INF004).

- Provisioning NFS and CIFS file shares (Access rights are managed by IKM officers and/or data owners).

- Enterprise storage & backup hardware and software procurement.

- Generally configured for high availability and dynamic resource allocation.

- Redundant SAN architecture via Dual-Fabric design.

Note: The Infrastructure Storage Services is provided through different data center levels in NCIA; Data Centers (DC), Enhanced Nodes (EN), Standard Nodes (SN), and Remote Nodes (RN) which depends on geographic location, network classification and capacity requirements. Not all features mentioned above are available in the four datacentre levels so during the requirements gathering the agency and customers shall mutually agree on the required features and hence the datacenter level is selected

Service Flavours: The Service is available as a single flavour

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret
Public Internet Access (PIA) Gateway

Service Prerequisites:

- INF001 LAN Service
- INF004 Infrastructure Virtualization Service
- INF005 Infrastructure Integration Service

Service lifecycle for storage devices:

The criteria for obsolesce for devices is defined by *NCIA's 10 year Lifecycle Plan*. According to this plan, life expectancy for storage devices is **'7'** Years unless the device is defined by the following criteria in order of urgency:

a. End of Service (EOS) devices
b. Failed of failing devices
c. Reported Missed SLAs as a result of failing devices
d. End of Life (EOL) devices

Standard Service Support Levels:

Service Availability Target: 99%

N.B. Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Reporting:

Incident management report base on ITSM tickets and trend analysis.

Change management and ASI report based on ITSM tickets.

Additional service reporting requirements can be requested through the respective SLAs which are subject to NCIA's cost and feasibility assessment.

Service Cost / Price: The service rate for this service is included under the service rate of INF004 Infrastructure Virtualization Service. No separate charges apply for this service specifically.

The unit of measure for INF004 is infrastructure unit (composed of Infrastructure Virtualization, Infrastructure Storage, Infrastructure Backup and Infrastructure Integration Services). The rate included in the INF004 service rate is for an average sized infrastructure unit (4 vCPU, 20GB vMemory and 850GB vStorage).

INF008 DCIS – DragonFly Service

The Service has been consolidated under the INF035 DCIS – Deployable Nodes Service.

INF009 DCIS – Limited Interim NATO Response Force (NRF) CIS-Expansion (LINC-E) Service

The Service has been consolidated under the INF035 DCIS – Deployable Nodes Service.

INF010 DCIS – Communications Gateway Shelters (CGS) Service

The Service has been consolidated under the INF035 DCIS – Deployable Nodes Service.

INF012 SATCOM Service

Service ID: INF012

Service Name: SATCOM Service

Portfolio Group: Infrastructure Services

Service Description: The SATCOM Service provides bandwidth to remote customers unable to be supplied by terrestrial infrastructure. The SATCOM infrastructure provides state-of-the-art communications supporting deployed operations anywhere within NATO's area of responsibility. It does this with its own ground equipment and control systems, operating with satellite capacity leased from the national governments of Great Britain, France, Italy and the United States.

Value Proposition: The Service provides the following value and benefits:

- **Location:** SATCOM services allow the customer to extend their communications networks to anywhere within NATO's area of responsibility.
- **Scale**: The service is scalable to support a variety of different deployments in both size and complexity, ranging from one telephone circuit to a complete intra-theatre hub and spokes and backhaul to the static HQ.
- **High redundancy:** The static SATCOM infrastructure has significant redundancy and a low probability of failure.
- **High Availability and Security:** SATCOM uses a variety of methods to ensure that communications in a hostile electronic environment maintains a high level of availability and security. These methods include:
    - Frequency hopping modems
    - Hardened satellites
    - Beam-nulling satellite antennas
    - Beam-steering satellite antennas

Service Features:

- **Redundant anchoring using dispersed locations:** provides greater resilience and availability, plus space diversity.
- **Dynamic bandwidth allocation** using global QoS to set priorities. Links are transparent to NGCS network.
- **Hardened satellites at X-band:** increased ability to work in a hostile electromagnetic environment.
- **Beam-nulling and beam-steering satellite antennas at X-band:** increased ability to work in a hostile electromagnetic environment.
- **Anti-jam modems:** increased ability to work in a hostile electromagnetic environment.
- **Voice and data services:** Links are transparent to NGCS.
- **Inherently secure communications** through the use of closed networks and the ability to integrate with VPN, COMSEC and TRANSSEC services. Increases security and integrity of information.

- **One-stop-shop** for all satellite queries and issues: NATO's centre of excellence for all SATCOM matters.
- **Fully managed communications suite** from an organization that understands the needs of the military. Centralised management ensures continuity, efficiency and full systems visibility.
- **Anchor station manning:** minimum one person on shift at all times to ensure timely response to faults, events and changing situations.
- **Ability to react quickly to new requirements** and changing circumstances: SATCOM is set up to process requirements within the SLA agreed with ACO.

Service Flavours:

Individual deployment: Small, commercial handheld and portable voice and low-speed data communications

Individual operational deployment: hand-held, vehicle and ship-mounted UHF systems providing secure, narrow-band voice and data. (Please note that the TACSAT UHF devices are separately captured under the INF040 UHF TACSAT Radio Services)

Wideband deployment: transportable systems providing voice, video and data to deployed formations, complete with intra-theatre and backhaul SATCOM networks using X- or Ku-band satellites

Wideband secure deployment: transportable systems providing voice, video and data to deployed formations, complete with intra-theatre and backhaul SATCOM networks using anti-jam modems and hardened X-band satellites

Additionally the table below provides infrastructure or support options available under each flavour, which cater to a variety of deployment requirements.

Service Flavour	Options under the Flavour	Description	in units	Support level available
Individual deployment	Inmarsat	Small, highly portable secure and insecure voice and data communications for initial deployments		2nd, 3rd line
	Iridium	Handheld telephone-type communications		2nd, 3rd line
Individual operational deployment	NUCC controller maintenance	This is the hub of the TACSAT system, providing DAMA and IW capabilities to improve bandwidth efficiency		2nd, 3rd line
Wideband Secure deployment	X-band anchoring	4 sites with 10 antennas to anchor all of NATO's broadband satellite communications, including anti-jam. Includes EMP assets	332MHz SAL-2 and 84MHz SAL-3	SAA production , 3rd line
	DCIS TSGT support	3rd-line maintenance, repair and upgrade management	As requested	3rd line

	DCIS DSGT support	3rd-line maintenance, repair and upgrade management	As requested	3rd line
Wideband deployment	SkyWAN operation and maintenance	Hub and spoke VSAT system, provided as VNC by LUX, currently used for NC2	2MHz, 8 terminals	2nd, 3rd line
	Melusina 2 administration	Administration of the LUX Ku-band VNC contribution	42MHz	3rd line
	DCIS TSGT support	3rd-line maintenance, repair and upgrade management	As requested	3rd line
	DCIS DSGT support	3rd-line maintenance, repair and upgrade management	As requested	3rd line

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

Service Prerequisites:

None

Standard Service Support Levels:

	Availability Target	**Service Restoration Period**
During Support hours	99.9 %	1 hour
Outside Support hours	99.5 %	4 hours

N.B. Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A0032	NATO SGS/SGT SAC Operator Maintainer
A0601	SATCOM Basic (048)
A4000	CCT200 SATCOM Terminal NATO Mission Iraq (NMI) Operator

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

INF013 Very Low Frequency (VLF) Broadcast Service

Service ID: INF013

Service Name: Very Low Frequency (VLF) Broadcast Service

Portfolio Group: Infrastructure Services

Service Description: Very Low Frequency (VLF) Broadcast services provide Submarine Operating Authorities (SUBOPAUTH's) with robust, secure and timely message delivery within the NATO Area of Responsibility in order to ensure effective Command and Control of sub-surface forces.

Value Proposition: VLF is the primary means of communicating with submarines. The NCI Agency managed VLF network is a key enabler for connecting shore SUBOPAUTH's to VLF Broadcast Radiating Stations for subsequent message delivery to submarines. The service additionally includes Broadcast Control Station (BCS) equipment which provides a live picture of the network status including; site status, keystream delivery and clear indication of system issues. Coupled with the ability to pass remote Over the Air Monitoring to a distance site and connection to external networks, this makes the BCS system extremely flexible for conducting submarine operations across NATO.

Service Features:

- Broadcast Control Authority (BCA)
  - Provides broadcast traffic at Mission Secret
  - System Management
  - Hardware and Software solutions
  - Interfaces with crypto for secure communications
  - Interfaces with Message Handling Systems (MHS)
- Broadcast Control Station (BCS)
  - Live connectivity picture
  - Broadcast Traffic Table management
  - Connection to NATO provided Broadcast Radiating Station (BRS) via the VLF network or to national transmitters via external lines.
  - Fully Redundant
  - Swap and replace solution
  - Facility to pass remote OTAM between sites
  - Group CHAT facility
  - Minimum operator involvement
- Broadcast Radiating Station (BRS)
  - Passes broadcast traffic to national transmitters
  - Utilises same hardware and software as BCS
  - Fully Redundant
  - Swap and replace solution
  - Minimum operator involvement
- NATO VLF WAN
  - NCI Agency managed dedicated IP network for VLF BCS
- Broadcast Support Site (BSS)

  - Provides test bed for system changes
  - Training facility

Service Flavours: The Service is available as a single flavour, with the following options:

- Complete end to end provision of VLF services (i.e. MHS to end user) or
- Individual or a mixture of the features listed.

Available on:

Mission Secret
NATO Unclassified

Service Prerequisites:

None

Standard Service Support Levels:

	Availability Target	**Service Restoration Period**
During Support hours	99.9 %	1 hour
Outside Support hours	99.5 %	4 hours

N.B. Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

INF014 Transmission Service

Service ID: INF014

Service Name: Transmission Service

Portfolio Group: Infrastructure Services

Service Description: The Transmission Service provides the network backbone infrastructure over wired or wireless transmissions bearers in order to connect all NATO Enterprise Static CIS nodes under a common Protected Core Community (PCC), underpinning the Network Enabled Capability of NATO. The Service is largely outsourced to 3rd parties (Commercial Service Providers and/or National Defence Networks NDNs). It includes full life-cycle service management like service design, capacity management, configuration and change management, operational support and continual improvement and optimization.

Value Proposition: The Service enables the NATO Enterprise static wide area network and provide the primary means by which dependent services and capabilities reach geographically dispersed consumers and users.

Service Features: The Service provides high capacity and resilient transport network infrastructure, scaled to meet the data traffic needs for all NATO Enterprise CIS nodes and future-proofed for additional customer requirements. It ensures effective transport of services and data across NATO by means of a Protected Core Network. The Service is comprised of the following elements:

Wired: delivered by fibre optic cabling as part of contract with Telecommunications Service providers or National Defence Networks (NDNs) providers. Available bandwidths:

- 100 Gbps
- 1 Gpbs or multiples
- 100 Mpbs or multiples
- Lower bandwidth based on requirements, costs and geographical constraints

Wireless: relatively short distance, where wired connectivity is not possible or efficient. Consists of links used to connect physically remote sites and come in the form of:

- Direct Line of Sight (DLOS): Microwave radio transmission equipment with directional antennas (100-400 Mbit/s), including CIP-67;

Service Flavours:

NATO Enterprise Static CIS nodes: Wired and wireless service elements are designed and offered as a bundle

3rd Party CIS nodes: Selectable elements out of the existing Service Features

Standard KPIs/KQIs:

Availability: Subject to external providers' SLAs and support contracts.

Available on: This service has no security classification and is considered as unclassified.

Service Prerequisites: None

Standard Service Support Levels: Service Availability for the Service is determined annually and is dependent on external support contracts, enabling services and regional support arrangements.

Available NCI Academy Training not covered by service cost:

A0236	NATO Networking Infrastructure (CCNA R&S)
A0650	CCENT (ICND1)
A3046	Network Configuration and Troubleshooting
A3135	Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR)
A3136	Implementing and Administering Cisco Solutions (CCNA)

Service Cost / Price: The unit of measure for the Service is 1 for Service Flavour of NATO Enterprise Static CIS nodes. For the 3rd party CIS nodes flavour, the unit of measure depends on the customer requirements and is calculated on an ad-hoc basis. The respective service provision cost is subject to external Service Provider contracts.

INF015 Broadcast, Maritime Rear Link and Ship-Shore (BRASS) STIV RMD Service

Service ID: INF015

Service Name: Broadcast, Maritime Rear Link and Ship-Shore (BRASS) System Test Integration and Verification and Reference Maintenance Diagnostic (STIV RMD) Service

Portfolio Group: Infrastructure Services

Service Description: The NATO Broadcast, Maritime Rear Link and Ship-Shore (BRASS) system is designed to support all NATO Maritime missions. It provides automated support for the NATO Maritime Surface Broadcast, the Ship-Shore and the Maritime Rear Link (MRL) HF communications networks**.** The System Test Integration and Verification and Reference Maintenance Diagnostic (STIV-RMD) facility replicates a minimal and representative BRASS operational site, mirroring the hardware and software components used in the BRASS Initial Core Capability, to the extent possible, with minimal additional hardware and software modules. The service includes all functions necessary to test and validate all services performed in an operational BRASS node. It is principally used for maintenance, testing and verification of BRASS software and its future implementations and is installed at Casteau Mons (SHAPE, Belgium), in NCIA facilities. The system can also be used for hands-on training of NATO/national BRASS personnel. The STIV-RMD facility interfaces the NGCS (NATO General Communication System) to connect to NCIA radio sites in The Hague and Staelduinen (NLD). The service is built from two nodes. One representing the standard BRASS node and the second allowing the simulation of the traffic up to the HF modem level. It is equipped with standard crypto units that are used in BRASS nodes and can be used in the simulation chains with unclassified traffic and crypto keys.

Value Proposition: The BRASS STIV-RMD facility allows testing of the key-streams transmitted/received by radios at the NCIA sites (HF TX in Staelduinen and the HF RX radio site in The Hague) without engaging assets required for military operations. The service design allows the simulation of the traffic without the need to use full radio equipment chains. The BRASS STIV-RMD facility is built in a manner similar to an operational system. The system processes, stores and disseminated unclassified data only and doesn't perform real operational activity, which makes STIV RMD a perfect tool to perform hands-on training for the NATO and national BRASS personnel.

Service Features:

- The system includes all functions necessary to test and validate all services performed in an operational BRASS node such as:
- Management of NATO/national Broadcasts, Ship Shore, MRL, MATELO and Point-to-Point circuits (STANAG 4285, STANAG 5066);
- Management of crypto equipment;
- Automatic storage and retrieval of message traffic handled in the centre;
- Remote control of the assets belonging to the system (including radio devices, antennae and communication links)

- The system includes the necessary hardware capacity and the full set of software tools required to maintain the BRASS software

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified

Service Prerequisites:

None

Standard Service Support Levels:

Service Availability Target: 98.0% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

INF016 Infrastructure Backup Service

Service ID: INF016

Service Name: Infrastructure Backup Service

Portfolio Group: Infrastructure Services

Service Description: The Infrastructure Backup Service is an underlying technical service that backs-up and restores (B&R) virtual machines (VMs) and server hosted files. This functionality offers automated and fully managed backup storage tenancy to customers (so that they can restore their data to active and inactive backup targets in case of technical or human caused failures, excluding disastrous events). This service provides the means to effectively manage backup data retention, long-term access and retrieval.

The service also delivers the functionality to restore data from previous copies in order to minimise the risk and impact of data loss caused by failures, human errors or data corruption. Retention period is specific to the different services and thus dependent on their specificities in terms of back-up requirements. The backup strategy for Customer Facing Services including retention time, backup type (full, differential), frequency/schedule (for transaction log backups), recovery model, restore time objective (RTO),recovery point objective (RPO) and other requirements can only be defined after in-depth coordination with the Customer regarding recovery objectives, acceptable risk, mission critical core services.

Value Proposition: The Infrastructure Backup Service:

- Enables the storage of multiple copies of data.
- Improves the ability to recover lost or corrupted data.
- Reduces the risk of losing critical data.
- Can facilitate data recovery from backups as required in the scope business continuity.

Service Features:

- Fully managed and automated data protection.
- Fully secured data access.
- In place or alternate location data restore capabilities.
- Flexible backup strategies.
- Crash-consistent backups.

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified;
NATO Restricted;
NATO Secret;
Mission Secret;
Public Internet Access (PIA) Gateway.

Service Prerequisites:

None

Standard Service Support Levels:

Service Availability Target: 99.0% Availability

Service Restoration: The Infrastructure Backup Service can restore VMs fully or partially. Restoring the entire service after a data restore is not in the scope of the Infrastructure Backup service. A yearly overview will be established for Customer facing services, focussing first on the top priority Functional (Application) Services identified in the ABIPAT table and where applicable indicating:

- Expected restoration times;
- Backup data retention scheme;
- Maximum data loss.

Data restoration: The time needed to restore data from backups varies based on the amount of data, location and available network throughput.

Data retention: By default, the data retention period is one month. However, upon request and coordination with the data owner, backup copies can be kept for a longer period.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The service rate for this service is included under the service rate of INF004 Infrastructure Virtualization Service. No separate charges apply for this service specifically.

The unit of measure for INF004 is infrastructure unit (composed of Infrastructure Virtualization, Infrastructure Storage , Infrastructure Backup and Infrastructure Integration Services). The rate included in the INF004 service rate is for an average sized infrastructure unit (4 vCPU, 20GB vMemory and 850GB vStorage).

INF017 DCIS – In-Theatre Mobile CIS Detachment (IMCD) Service

The Service has been consolidated under the INF035 DCIS – Deployable Nodes Service.

INF018 DCIS – Mini Point of Presence (Mini-PoP) Service

The Service has been consolidated under the INF035 DCIS – Deployable Nodes Service.

INF019 DCIS – Theatre Liaison Kit (TLK/ILK) Service

The Service has been consolidated under the INF035 DCIS – Deployable Nodes Service.

INF020 DCIS – Deployable CIS Equipment Pool (DCEP) Service

Service ID: INF020

Service Name: DCIS – Deployable CIS Equipment Pool (DCEP) Service

Portfolio Group: Infrastructure Services

Service Description: DCEP consists of standard desktop terminal equipment that provides Communications Information Systems (CIS) Services to support the end user in the deployed environment. This equipment includes classified and unclassified workstations and laptops, classified (VoSIP) and unclassified (VoIP) telephones, projectors, printers, scanners, multi-function devices (MFD), VTC terminals, multi-point voice conference devices, large screens and workstations with multi-screen capability. DCEP also contains an SLA specific amount of user equipment to support the Core Geographical Information Services (Core GIS) user community.

The service rate includes the cost for shipping NATO Reaction Force(NRF) DCEP equipment between the level 3 storage/repair facility and Customer peacetime locations, including the rotation of NRF assigned equipment between Customer locations when no return to repair centre is required.

INF020 funding covers the level 3 maintenance, repair and replacement of faulty equipment therefore assuring the availability of the service at NCISG NSBs and NCI Agency CSSC.

LOG005 service funds the DCEP exercise support; preparation, deployment shipping, re-deployment shipping, level 3 testing, repair costs, cleaning and storage.

Operational tasking and assignment of all assets within the Service is the responsibility of the ACO J6 Cyber Operations Centre. This includes the allocation of DCEP starter packs to NCISG NRF Standby DCIS Systems to pre-approved quantities.

Value Proposition: DCEP is a fully common funded DCIS capability that is available for use by the entire NATO Command Structure in support of Missions and the Medium Term Exercise Plan (MTEP).

This Service provides all hardware to extend NCI Agency Services hosted on DCIS NDDs and/or MIR to the Users community assigned to the Mission and Exercise Domains as per the Customer's business needs.

Management: The Provider includes Service Management support to the customer, as well as being the primary NCI Agency interface and initial point of contact with the customer for in year execution of the services in accordance with the Service Level Agreement (SLA). The Service Management support includes the management and coordination of service deliverables across all NCI Agency entities.

Service Features:

Service Delivery Management (SDM): DCIS services are specific with the requirement for close coordination between Service Provider and the Service Operator. For that purpose, Service Delivery Schedule and Change Management Plan as planning and coordination tools are used and updated on a monthly basis. SDMs also provide Service Availability Management and Service Obsolescence Management Reports.

Service Provision: DCEP Service provides end user devices that can connect to MS, NS and NU domains for the deployed HQ staffs. In addition, DCEP service provides the NDD DCIS operator (crew) and DCIS system administration laptops.

End User Device connection to and disconnection from the DCIS domain is via an ITSM Service Request submitted to the Enterprise Service Operation Centre.

DCEP Service Maintenance:

- Level 1 and Level 2 equipment maintenance is conducted by the Customer at Peace Time Location (PTL) or deployed.
- The Provider delivers Centralised level 3 maintenance at CSSC Brunssum, at DCEP PTL or deployed locations.
- The DCEP Service does not include IT consumables to the DCIS user. Consumables items, for example, printer toner, printer paper, batteries, cleaning products, headsets are the responsibility of the Customer and should be procured locally.

Service Flavours:

CIS Assets/Services: Standard DCEP Assets and Quantity		Min Specifications	Standard Ancillaries	Remarks
Laptop (INF020-1)	3,300	Dual Core Processor, 8Gb RAM, 100Mbps NIC, HD Graphics, 256Gb HDD/SSD, WIN 10 20H2 compatible with Windows Experience Index (WEI) Value > 4 on Processor, Disk Drive, Graphics and RAM	Power Supply	Hardware only - Enables user access to Classified and Unclassified data networks and services. Software/drivers are provided by the Customer as per current NRF Windows 10 Baseline
Work Station/ Computer (INF020-2)	1,300	Dual Core Processor, 8Gb RAM, 100Mbps NIC, HD Graphics, 256Gb HDD/SSD, WIN 10 20H2 compatible with Windows Experience Index Value of 4 or greater on Processor, Disk Drive, Graphics and RAM	Power cable, monitor, video cable, keyboard, mouse	Hardware only - Enables user access to Classified and Unclassified data networks and services. Software/drivers are provided by the Customer as per current NRF Windows 10 Baseline
Monitor (INF020-3)	2,750	20-24" colour monitor, 1600x900 resolution with range of VGA, DVI, DP, HDMI output options, WIN 10 20H2 compatible	Power cable, video cable	Hardware only - Enables users to have single and dual screen monitors on workstations and laptops on Classified and Unclassified networks. Software/drivers are provided by the Customer as per current NRF Windows 10 Baseline
Printer/ MFD (INF020-4)	750	A3/A4 Colour or Black & White Laser printer. Network or Stand Alone options via RJ45 or USB connectivity, WIN 10 20H2 compatible	Power cable, 1 set toner cartridges, USB/Network cable	Hardware only - Enables users to Print / Copy / Scan from A4 B/W up to A3 colour. Software/drivers are provided by the Customer as per current NRF Windows 10 Baseline
Scanner (INF020-5)	60	A4 Colour, 2400x2400 DPI, WIN 10 20H2 compatible	Power cable, USB cable	Hardware only - Enables users to scan A4 colour copies on Classified and Unclassified networks. Software/drivers

				are provided by the Customer as per current NRF Windows 10 Baseline
VoIP Phone (INF020-6)	2,150	CISCO 7900 and 8400 series VoIP and VoSIP telephones. 100Mbp RJ45 or FO connectivity	Power cable (if required), network cable	Hardware plus CISCO ios only - Enables user access to classified or unclassified telephony services. Configuration is provided by NCIA as system is configured from Node State to Mission State
VTC Equipment (INF020-7)	45	Polycom Video Teleconference System POLYCOM, REAL PRESENCE,GROUP 500-720P	As per System manuals	Hardware plus Polycom RealPresence VTC software - Enables user access to Classified and Unclassified Video Teleconferencing services. Configuration is provided by NCIA as system is configured from Node State to Mission State
Projector/ Beamer (INF020-8)	120	1500LM, 1024X768, 4:3 aspect ratio, c/w range of AUDIO/HDMI/RCA/VGA/USB output options	Power cable, video cable	Hardware only - Enables conference room and briefing room services to be displayed
Projecting Screen	80	180cm x 180cm screen	Transit tube	Hardware only - Used with projector/beamer
Switch (INF020-9)	270	Full duplex, Layer 2 OSI device, 24 or 48 x 100Mbps access ports, 2 or 4 x 1Gbps uplink ports, WIN 10 20H2 compatible	Power cable	Hardware plus CISCO ios only - Provides Layer 2 access level connectivity for end user Data devices on Classified and Unclassified networks. Configuration is provided by NCIA as system is configured from Node State to Mission State
Fibre Reel (INF020-10)	270	Tactical fibre optic, 250 meters, single mode duplex.		Hardware only tactical fibre cable. HMA tactical connectors, single mode 9/125 micron, 250 metres on reel.
KVM Switch (INF020-11)	1000	Tempest level C. Supports up to 2 host computers and 2 displays. Data leakage prevention between connected computers		2nd Gen Universal, secure KVM switch, 2-port dual head
CIS Assets/Services: Core GIS DCEP Assets[1]		**Min Specifications**	**Standard Ancillaries**	**Remarks**
Core GIS Kit: Generation 1/3 (INF020-12)	8 16 6 6	DELL Precision 3620, Dual Core Processor, 8Gb RAM, 1000Mbps NIC, HD Graphics, Tempest C, Removable 500Gb HDD, WIN 10 20H2 compatible 23.8" HP Elite Display E240 colour monitor, WIN 10 20H2 compatible HP M880Z A3 Colour Multi-function printer. Network or Stand Alone options via RJ45 or USB connectivity, WIN 10 20H2 compatible HP Designjet T830-36 A0 Colour plotter. Network or Stand Alone options via RJ45 or USB connectivity, WIN 10 20H2 compatible HP Designjet T520 A1 colour plotter. Network or Stand Alone option via RJ45/USB, WIN 10 20H2 compatible	Transport case, Power supply, keyboard, mouse Power and video cables Power cable, 1 set toner cartridges, USB / Network cable Power cable, 1 set ink cartridges, USB / Network cable	Hardware only - Enables user access to Core GIS data networks and services. Software/drivers are provided by the Customer as per current NRF Windows Core GIS Baseline Hardware only - Enables users to have single or dual screen monitors on Core GIS workstations. Software/drivers are provided by the Customer as per current NRF Windows Core GIS Baseline Hardware only - Enables users to Print / Copy / Scan from A4 B/W up to A3 colour. Software/drivers are provided by the Customer as per current Core GIS Baseline Hardware only - Enables users to Print up to A0 colour. Software/drivers are

[1] Core GIS assets are included in the DCEP portfolio of individual equipment items but are designed to be deployed only as complete Core GIS kits.

	6 4 24	Disk Array, Synology DS918+, 4 bay, 2.5/3.5", ESATA/2X RJ45/USB 3.0, INTEL CELERON J3455 2.3GHZ, 4GB RAM, WIN 10 20H2 compatible External Hard Disk Drive, 3.5", USB 3.0, 8TB, SEAGATE Backup Plus Hub, 160MBPS	Power cable, 1 set ink cartridges, USB / Network cable Power cable, USB / Network cable Power cable, USB / Network cable	provided by the Customer as per current Core GIS Baseline Hardware only - Enables users to Print up to A1 colour. Software/drivers are provided by the Customer as per current Core GIS Baseline Hardware only - Enables users to externally store, backup and transfer data inside or outside of the network. Software/drivers are provided by the Customer as per current Core GIS Baseline Hardware only - Enables users to externally store, backup and transfer data outside of the network. Software/drivers are provided by the Customer as per current Core GIS Baseline
Core GIS Kit: Generation 2 (INF020-13)	14 28	Dual Core Processor, 16Gb RAM, 100Mbps NIC, HD Dual Screen Capable Graphics, 512Gb HDD/SSD, WIN 10 20H2 compatible. 23.8” HP Elite Display E240 colour monitor, WIN 10 20H2 compatible	Transport case, Power supply, keyboard, mouse Power and video cables	Hardware only - Enables user access to Core GIS data networks and services. Software/drivers are provided by the Customer as per current NRF Windows 10 Core GIS Baseline Hardware only - Enables users to have single or dual screen monitors on Core GIS workstations. Software/drivers are provided by the Customer as per current NRF Windows Core GIS Baseline
DF BoB	18	Full duplex, Layer 2 OSI device, 24 x 100Mbps access ports, 2 x 1Gbps uplink ports	Power cable	Hardware plus CISCO ios only - Provides Layer 2 access level connectivity for end user Data devices on Classified and Unclassified networks. Configuration is provided by NCIA as system is configured from Node State to Mission State
Media Convertor	508	Range of 10/100/1000Mbps, RJ45 to LC/SC/SFP	Power supply	Hardware only - Enables conversion of CAT5e/CAT6 copper cable to Multimode Fibre Optic cable
Webcam	150	2.0 Megapixel, Wide Angle 1280x1024 resolution, HD webcam with USB IP connectivity and built-in microphone		Hardware only - Enables user access to video and audio services on workstations and laptops. Software/drivers are provided by the Customer as per current NRF Windows 10 Baseline

Configuration Changes:

- Major – Defined as a significant change to the service, such as complete replacement of all or majority of key configuration items. Major Changes are outside of the scope of the service and are managed through the NATO Security and Investment Program (NSIP).

- Minor – Defined as low risk, continuous routine housekeeping such as minor software maintenance, hardware updates, security updates, and patches and replacement of defective equipment. Minor Changes are conducted continuously throughout the lifecycle of the Service and are undertaken by the Provider without affecting operational availability.

Service Prerequisites: User provided qualified operators.

Standard Service Support Levels:

Service Availability Target: In accordance with the stipulations of the service provisioning agreement and based on the Customer requirements.

Service Restoration Period: In accordance with the stipulations of the service provisioning agreement.

Service Cost / Price: The unit of measure for the Service is per item.

INF021 DCIS – Third Generation Transportable Satellite Ground Terminal (TSGT) and Upgraded Transportable Satellite Ground Terminal (UTSGT) Service

The Service has been consolidated under the INF036 DCIS – Deployable SATCOM Service.

INF022 DCIS – Deployable Satellite Ground Terminal (DSGT) Service

The Service has been consolidated under the INF036 DCIS – Deployable SATCOM Service.

INF023 Contingency Network Service

Service ID: INF023

Service Name: Contingency Network Service

Portfolio Group: Infrastructure Services

Service Description: The Contingency Network Service manages provisioning and delivery of the contingency network connections, encompassing lifecycle stages from requesting the network connections until their retirement in an orderly and well-defined fashion. It comprises of the provision of simple network connections, normally used as ship connections or simple deployable asset reach-back connections for deployable network services in operations and/or exercises. The Service is available only to non-common funded customers of the NCI Agency.

Value Proposition: The Service enables an efficient establishment of temporary connections to the NATO Enterprise network and a temporary access to various NCI Agency IT services.

Service Features: The Service streamlines and tracks all the essential network service-provisioning activities such as requesting, funding/eligibility validation, design, configuration management, implementation, testing, and service operation.

Service Flavours: The Service is available in two flavours:

1. Establishment/modification of a contingency network connection;
2. Activation/deactivation of an existing contingency network connection.

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

Service Prerequisites:

None

Standard Service Support Levels: N/A

Available NCI Academy Training not covered by service cost:

A3046	Network Configuration and Troubleshooting

Service Cost / Price: The unit of measure for the Service is Per Connection. Price details available in the Service Rate document.

INF024 DCIS – High Frequency (HF) Service

The Service has been consolidated under the INF037 DCIS – Deployable Radio Transmission Service

INF025 DCIS – Deployable Line of Sight (DLOS) Service

The Service has been consolidated under the INF037 DCIS – Deployable Radio Transmission Service.

INF026 DCIS – Deployed Operational Gateway (DOG) Service

The Service has been consolidated under the INF038 DCIS – Deployable Nodes Anchor Service.

INF027 DCIS – Mission Preparation Centre Service

The Service has been consolidated under the INF038 DCIS – Deployable Nodes Anchor Service.

INF028 ACCS Sensor Integration Module (ASIM) Service

Service ID: INF028

Service Name: ACCS Sensor Integration Module (ASIM) Service

Portfolio Group: Infrastructure Services

Service Description: The ACCS Sensor Integration Module (ASIM) is an information conversion service that facilitates the integration of civilian and military sensors with AirC2 systems like ACCS (APP050) or MASE (APP053). ASIM enables this integration of legacy civilian or military air defence sensors by translating a variety of sensor formats to an STANAG 5535/ADatP-35 or EUROCONTROL ASTERIX conform protocol as used by the AirC2 system.

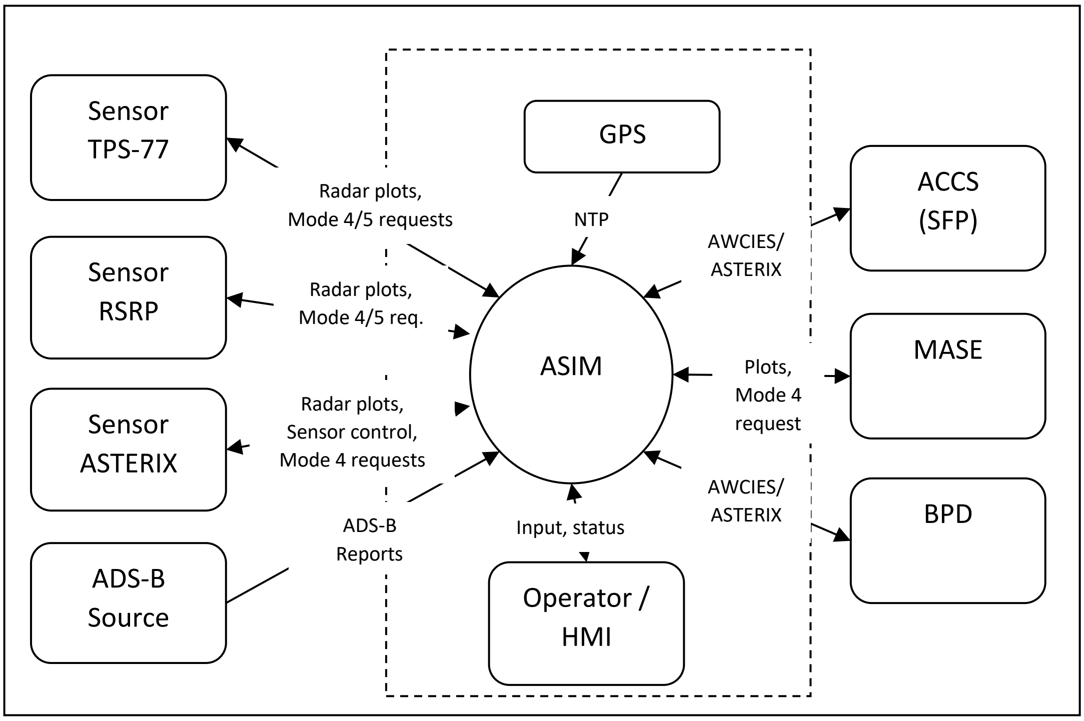
ASIM receives and converts sensor data, i.e. plots, strobes and radar status messages into equivalent ADatp-35 or ASTERIX conform messages and forwards this to the AirC2 system processing when applicable. Working the opposite direction as well, radar control and status information from AirC2 systems is translated respectively and forwarded to the connected sensors. Additionally, ASIM automatically provides sensor status data required by ACCS to declare the sensor link operational.

Value Proposition: ASIM Service provides a standard solution for interfacing non-compliant sensors with AirC2 ACCS (APP050) and MASE (APP053). The translation and exchange of data is fully configurable, automated and does not require operator attention. ASIM enables data to be monitored and controlled while sensor and control data can be recorded, replayed and dumped in real-time for quality analysis.

Service Features:

- ASIM connects legacy sensors with ACCS and MASE and provides target reports.
- Radar control actions from the ACCS/MASE operator are translated into sensor-specific messages, when applicable. I.e. currently Mode 4 and Mode 5 requests;
- The exchange of data is fully automated and does not require operator attention.
- The ADatP-35 and ASTERIX data into and out of ACCS or MASE can be recorded, replayed and dumped in real-time for data reduction and analysis;
- Redundancy as required for ACCS is supported;
- Safety related events are also forwarded to ACCS by ASIM as radar failure reports.
- Sensor and control data translation with a minimum latency and throughput not less than what is required for ACCS or MASE;
- In principle, ASIM appears to both ACCS/MASE and sensor as a transparent system. However, if target reports have an inconsistency between time and azimuth (which can lead to reduced tracking performance of the connected C2 system), ASIM is able to reduce this error based on reference data from the sensor.

The figure below outlines ASIM in a typical use case:



Supported configuration

- ASIM typically consists of two servers able to separate the sensor interface from the AirC2 system interface. This two-server configuration also supports to handle security levels differences between sensor groups and the AirC2 system.
- A boundary protection system such as the Application Layer Firewall for Sensors and Flight Plans (ALF-SFP – SEC022) can be integrated with the ASIM installation to protect system security boundaries from cyber threats.

Supported sensor/interface standards:

ASIM is STANAG 5535/ADatP-35 compliant towards the sensor and the AirC2 system and supports various sensor data formats inclusive JASR8, RMP, DDL, (A)S29, RAT31DL, FPS 117, TPS77, HADR, CD2, RSRP, S743D, AWCIES, T101, Cardion, T92, SRT and EUROCONTROL ASTERIX (various).

Other hardware, software and CIS details

- Uses NCI Agency (NPC) Integrated Solaris platform (NISP) as a secured Solaris OS platform
- X86 or SPARC based server HW able to run NISP/Solaris

Service Flavours:

ASIM supports service the following service flavours:

- **NCS wide NATO ASIM** single SW baseline maintenance and In-Service-Support (ISS). The NATO ASIM SW baseline maintained with this service flavour is a prerequisite for all other service flavours.

- **Single ASIM configuration**, direct interfaces to sensor data and the ASIM servers are installed at a single location, usually at the ACCS location.
- **Split ASIM configuration** supports geographical separation of the direct sensor interfaces from the ASIM server connected directly to ACCS. This also supports that multiple remote sensor interface servers can connect to one server which provides the data to ACCS. This ASIM service flavour might be used to build up sensor networks managing the sensor data distribution between multiple sensors, AirC2 and ATC centres.

These two service flavours can be combined with an Application Layer Firewall for Sensors and Flight Plans (ALF-SFP – SEC022) to protect to protect system security boundaries against cyber threats.

Available on:

NATO Unclassified for handling civilian sensor data;
NATO Confidential for handling military sensor data and
NATO Secret for directly interfacing with the AirC2 system.

Service Prerequisites:

PLT013 (former APP051) NATO Integrated Secure Platform (NISP) platform service – mandatory – provides the secured operating system platform for hosting the ASIM server applications.

SEC022 – Application Layer Firewall for Sensors and Flight Plans (ALF-SFP) Security Service – optional – provides boundary protection serves for connected AirC2 systems.

ASIM Hardware, software and connection requirements:

- Serial to IP network converter for serial sensor data;
- Sensor data available as serial data or at IP network level;
- IP interface as part of the ACCS or Air C2 system
- Server hardware compatible to run PLT013 - NISP and authorized to host the ASIM at required security level.
- Network infrastructure

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

- Monday to Thursday: 0600 to 2200 (CET)
- Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 CET).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

- Belgium +32 65 44 3177
- Netherlands +31 70 374 3177
- Italy +39 081 721 3177
- Germany +49 282 4978 3177
- USA +1 757 747 3177
- For NATO HQ +32 02 707 5858

Service Requests:

To request the INF028 - ASIM service, please complete the Customer Request Form and contact NCI Agency through the submit function included in the form following the link below. https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

Functional unit	Service Level Target (availability)	Performance Thresholds
ASIM in single and split configuration	99.5%	30 ms delay for passing data between sensor and Airc2 system

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Available NCI Academy Training not covered by service cost:

A1010	ASIM System Administrator

Service Cost / Price: The Service delivery cost for each flavour is charged in accordance with specifically arranged conditions of the Service delivery.

Service ID	Service Name	Service Flavour/Option	Service Unit of Measure
INF028	ACCS Sensor Integration Module (ASIM) Service	NCS wide ASIM software baseline maintenance and In Service Support (ISS)	1
INF028	ACCS Sensor Integration Module (ASIM) Service	Single ASIM configuration	1
INF028	ACCS Sensor Integration Module (ASIM) Service	Split ASIM configuration	1

INF029 NATO High Frequency (HF) Support Service

Service ID: INF029

Service Name: NATO High Frequency (HF) Support Service

Portfolio Group: Infrastructure Services

Service Status: Available

Service Description: The High Frequency (HF) Support Service is mainly provided via NATO BRASS (Broadcast, Ship-Shore) system, which is designed to support all NATO Maritime missions. The Service provides automated support for the NATO Maritime Surface Broadcast, the Ship-Shore and the Maritime Rear Link (MRL) HF communications networks and timely, accurate and reliable command and control communications and information exchange with NATO message switching and distribution capabilities.

There are NATO and nationally owned BRASS stations. National stations offer BRASS services to NATO based on Memoranda of Understanding signed with ACO. During the development, implementation and in-service support of NATO BRASS, NCI Agency has gained invaluable knowledge and is offering:

- Budgeting and financial mechanism to manage NATO funds granted for BRASS services delivered to NATO by Nations.
- In service support to BRASS Automated Control and Management Systems (ACMS).
- Support for BRASS Initial Core Capability (ICC) software.

Value Proposition: The HF Support Services offered for BRASS System provide:

- Proficient budgeting and financial structure in place with know-how of NATO procedures.
- Long experience gained during the in-service support of NATO BRASS sites.
- Expertise on the BRASS ICC software supported by the capabilities of the BRASS System Test Integration and Verification and Reference Maintenance Diagnostic (STIV RMD) facility located in NCIA Mons.

Service Features: The main features of NATO HF Support Services are:

- Existing budgeting and financial mechanism to manage NATO funds granted to pay for BRASS services delivered to NATO by Nations. In the past, NCIA managed funds for HF services delivered by Portugal to NATO and may provide similar support to ACO in case of Nations offering BRASS services to NATO based on service provision approach.
- In service support to BRASS Automated Control and Management Systems (ACMS). NCIA was managing the NATO ACMS nodes and HF stations before they were handed over to the Host Nations. NCIA supports the NATO ACMS in Northwood.
- Support for BRASS Initial Core Capability (ICC) software for the Nations that use it and may decide to use it in the future. The software baseline and source code and documentation is available for free to NATO nations. BRASS ICC software support and maintenance activities are performed in the NCIA BRASS System Test

Integration Verification Reference Maintenance and Diagnostic Facility (STIV RMD).

Service Flavours: This Service is available as a single flavour.

Available on: NATO Unclassified

Service Prerequisites: None

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

INF032 DCIS – Small Deployable Military Bandwidth SATCOM Terminal (DMBST) Service – BBSST & DART Terminals

The Service has been consolidated under the INF036 DCIS – Deployable SATCOM Service.

INF034 Recognized Air Picture (RAP) Dissemination Service

Service ID: INF034

Service Name: Recognized Air Picture Dissemination Service

Portfolio Group: Infrastructure Service

Service Status:

L1DDN flavour: Available
Secure RAP flavour: Pipeline

Service Description: The Recognized Air Picture (RAP) Dissemination service primarily provides the infrastructure for transporting unencrypted Link 1 Data from the originating head end over NGCS network to the terminating tail end where the Link 1 Data is required. The Service is defined as the provision of infrastructure assets and capacity that enables the user to establish defined point-to-point connectivity. Secure RAP flavour is yet to be fully defined once the pipeline phase has completed. Secure RAP is geared towards providing the transporting of secure Link 1 Data and other required protocols references in Minimum Military Requirements (MMR) from the customer and AIRCOM mission.

Value Proposition: The Service is an integral component enabling the simultaneous transport and distribution of the Link 1 Data the Command and Reporting Centres (CRC), Combined Air Operations Centres (CAOC), and the Static Air Defence Centre (SADC), as well as for cross border connections CRC-to-CRC. Simultaneously, the service also enables the transport of Air Command and Control System (ACCS) data and Voice Loop (VL) services. Link 1 data enables the production of Recognized Air Picture (RAP), which, along with ACCS and VL are critical to the mission of AIRCOM.

Service Features: The L1DDN flavour services are available in the black domain of NGCS with the extended infrastructure elements to the CRC locations. L1DDN enables the transport of unencrypted Link 1 data, VL and ACCS data delivery. Secure RAP shall enable the secure transport of Link 1 data and ACCS data delivery.

Service Flavours:

L1DDN – enables the transport of Link 1 data between National CRCs and enables X-Border interconnections for same data exchange. The data exchanged and transported through the L1DDN is represented by Tactical Data Link (TDL) Link 1, operational Voice Loop services, and in some specific cases ACCS data. The Service is provided by leveraging and having dependencies on the capabilities delivered via NATO General Purpose Communication System (NGCS) available at the national NGCS Point of Presence (POP) and the National Defence Networks. The L1DDN is operational across all 30 NATO Nations, with presence and interconnections[1].

Secure RAP – distribution capability currently being implemented. A number of sites are planned start to distribute their Link 1 data or similar protocols via the secure links.

[1] As defined in AD 80-7 Vol III

The other will be integrated as the implementation project progresses in the following years. L1DDN should be decommissioned after the Secure RAP distribution is fully operational.

Available on:

L1DDN – NATO UNCLASSIFIED
Secure RAP – NATO SECRET

Service Prerequisites:

L1DDN flavour:

- INF014 Transmission Service;
- INF002 NGCS PoP Service;
- Transmission services via commercial or NDN providers between the CRC and the NGCS POP in the Nation.

Secure RAP flavour:

- INF014 Transmission Service;
- INF002 NGCS PoP Service;
- Transmission services via commercial or NDN providers between the CRC and the NGCS POP in the Nation.
- Pico PoP/POP required at all endpoints.

Standard Service Support Level:

Hours of support	24h/7d for CSD, 8h/5d for SLS/TLS

Service Availability Target: Service Availability for the Service is determined annually and is dependent upon enabling services and regional support arrangements. Service availability cannot be higher than the one of any of the enabling services.

Service Restoration:

Response time	1 hour
Restoration time	1d (critical/high), 3d (medium)

Available NCI Academy Training not covered by service cost:

A3046	Network Configuration and Troubleshooting
A3136	Implementing and Administering Cisco Solutions (CCNA)

Service Cost/Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

INF035 DCIS – Deployable CIS Nodes Service

Service ID: INF035

Service Name: Deployable CIS Nodes Service

Portfolio Group: Infrastructure Services

Service Description: This Service provides Standardised and Certified Deployable Communication and Information Systems (DCIS) Nodes. The Service provides the infrastructure and platform for a deployable CIS capability with inherent characteristics of modularity, scalability, sustainability, and interoperability. Each customer can adapt the Service to meet specific operational requirements through selection of the required workplace and application services. The customer can select those services from the workplace and application services sections of the Customer Costed Service Catalogue.

The Service includes service monitoring and reporting. This service has been upgraded in 2024 with the addition of enhanced cyber defence capability.

Value Proposition:

In peacetime location the service enable NATO to demonstrate a high readiness posture.

When deployed, the services enable NATO Warfighters to make the timely decisions for Mission Success.

The customer will have direct access to the Agency Service Management team for Deployable CIS and will be supported as described in the OTH004 Service Description.

Service Features:

Included NCI Agency Services: listed for each specific flavour in the Service Flavours section.

Included NCI Agency Services correspond with standard NCI Agency services, as described in respective service definitions. However, due to deployable nature of the entire DCIS Nodes Service, features of these services may differ from the standard ones, and standard flavours and service support levels may be not applicable. Where required, these differences will be described in detail within the respective service provisioning agreement (i.e. SLA, SSP, TA, etc.). Delivery cost of these services differs from the standard service rates, and it is entirely included within the DCIS Nodes Service cost.

The DCIS Nodes Service can host a variable number of Users (workplace services) and Application Services (Functional Area Services, FAS). The customer can select the specific requirements for the workplace and application services using the service catalogue, at additional cost.

Included in the service rates are the workplace services and applications for the system administrators to perform their duties.

Included CIS Assets: listed for each specific flavour in the Service Flavours section.

Included Non-CIS Assets: listed for each specific flavour in the Service Flavours section.

Reporting: Manually generated, no automated 24/7 monitoring of the Service status/availability is feasible.

Configuration Changes:

Major – Defined as a significant change to the service, such as complete re-configuration of all or majority of key configuration items (change of the service baseline), primarily in order to prepare a service for a new mission. The standard change of the service baseline, costed as one complete change every two years. The schedule of Major Changes are agreed by both Provider and Customer in advance. The configuration baseline is made available to the customer through the Configuration Management Database.

Minor – Defined as low risk, continuous routine housekeeping such as minor software maintenance, security updates, and patches. Minor Changes are conducted continuously throughout the lifecycle of the Service, undertaken by the Provider without affecting operational availability.

Configuration and maintenance of the backup capability included.

Maintenance:

Preventative Maintenance Inspections (PMI) – The PMI to the Service are conducted at support Level 3 (L3) and in coordination with Customer to take into account the impact on operational availability and requirements, as a standard, along with configuration changes schedules taking into account manufacturer's instructions on maintenance, or otherwise defined technical maintenance standards;

Corrective Maintenance Inspections (CMI) – CMI is undertaken by Provider in the event of Service asset failure, at support Level 3 (L3) and in accordance with the Customers' requirements as described in the service provisioning agreement. This includes replacement of non-reparable equipment, where applicable under NATO financial rules and regulations.

Maintenance includes regular sustainment of used applications and related licenses.

Shipment and transportation: Service assets will be provided at Customer's disposition at any of customer's permanent locations. Full shipping between the repair- and peacetime location is included.

Documentation: Customer will be provided with required technical documentation, as specified in the service provisioning agreement.

Spare parts: Service includes required stock of support L1 and L2 spare parts, as specified in the service provisioning agreement. L1 and L2 spares are delivered to the Customer baselined at the factory state. Provider holds sufficient spares needed for Agency scheduled maintenance and anticipated incident resolution at the level to meet the service KPIs. Local users hold L1 spare parts in accordance with recommended spare part list provided in the specifications for each system. Local users are responsible to request replenishments trough Provider's Material Request Procedure.

Security Accreditation Documentation: Customer will receive prepared documentation required for the Security Accreditation.

Signal Support Group Cyber Defence Toolkit (SSG CDT) (SEC021):

Available as an option to specific flavours, as specified in the Service Flavours section. The feature supports a Deployed Network Operations Centre (DNOC) of a JFC Commander by providing a single deployable Cyber Defence Toolkit (SSG CD Kit) for monitoring the NU domain against intrusion.

Customer personnel operate the SSG CD Kit from the DNOC by adhering to all relevant NATO cyber defence related policies and processes. In the event that the cyber service is impacting the delivery of services to the user community, the provider will inform the customer and the service will be terminated immediately.

The SSG CDT feature entails:

- L3 engineering support;
- Microsoft standard software support to successfully detect malicious traffic, email attachments, SQL injection attacks, denial of service attacks, and other cyber threats; and
- Provision of the following security services: Cyber Security Incident Management Service (SEC006), Cyber Security Monitoring Service (SEC007), Cyber Security OPCEN Helpdesk Service (SEC008), Cyber Security Outreach Service (SEC009), Cyber Security Information Sharing Service (SEC010), Gateway Security Service (SEC011), and CIS Protection Support Service (SEC012).

There are the following assets included in this feature:

- CIS Assets: DNOC SIEM Server, Sensor Workstations, Eclypt Hard Drive (HDD), Eclypt External Hard Drive (HDD), Eclypt Hard Drive (HDD) Management, VPN/Firewall, VPN Concentrator/Firewall, and Network Taps (Datakom);
- Non-CIS Assets: General Purpose (GP) Tents, Environmental Control Unit (ECU), UPS, Racks, Power Strips.

Additional Options: listed for each specific flavour in the Service Flavours section.

Service Flavours: The flavours of the Service are designed with different capabilities to effectively meet all operational scenarios. Each flavour includes additional options to enable full adaptation of the Service to the operational requirements. Options are to be requested by the customer through the annual submission of the requirements changes, in accordance within the established and/or agreed requirements establishment and budgeting process. Any in-year change of options shall be dealt with in accordance with the procedures agreed within the service provisioning agreement. Costing of options is conducted on per request basis.

The flavours of the Service are:

DragonFly (INF008) – a 3 domain system integrated into transit cases, full FMN and NRF compliant. Can operate self-sustained without reach-back to the data centre, provides standard user services and can host full set of FAS applications, supports up to 192 users per domain. Interconnects using X-Band SATCOM, digital line of sight, military or commercial landline. The service is provided with non CIS assets; tents, BC protection, and ECU, UPS and manual handling equipment to enable operation in harsh environments between -30° and +49° Celsius. The Service provisions the user equipment for 30 users and can be augmented by the DCEP Service (INF020) to bring it up to 192 users.

Communications Gateway Shelters (CGS) (INF010) – a 3 domain, shelter based system, that can operate self-sustained without reach-back to the data centre, provides standard user services and capable of hosting full set of FAS applications. It supports up to 250 users per domain. Interconnects using X-Band SATCOM (INF037), High Capacity Digital Line Of Sight (INF026), and military or commercial landline. The Service is provided with non-CIS assets, such as: shelters (CIS, crypto maintenance and system administration), ECU, UPS, and generators to enable operation in harsh environments between -30° and +49° Celsius. The CGS Shelter is transportable on any transportation equipped with TWIST-locks for 20-ft ISO Containers, including road, rail, cargo ship, and cargo aircraft means of transportation. The Service provisions the user equipment for 30 users and can be augmented by the DCEP Service (INF020) to bring it up to 250 users.

Limited Interim NRF CIS – Expansion (LINC-E) (INF009) – a 3 domain system integrated into transit cases, meets NRF requirement for low intensity operations but not FMN compliant as an interconnection node (no INM), can operate self-sustained without reach-back to the data centre, provides standard user services and capable of hosting a limited set of FAS applications (to be specified in the SLA), supports up to 126 users per domain. Interconnects using X-Band SATCOM, digital line of sight or military landline. The Service is provided with non-CIS assets: light cargo vehicles, tents, ECU, UPS, and generators to enable operation in harsh environments between -30° and +49° Celsius. The Service provisions the user equipment for 30 users that can be augmented by the DCEP Service (INF020) to bring it up to 126 users.

In-Theatre Mobile CIS Detachment (IMCD) (INF017) – a 3 domain system integrated into transit cases capable of supporting low intensity operations, does not meet the requirements of NRF (not C130/C160 RORO) and not FMN compliant as an interconnection node, can operate self-sustained without reach-back to the data centre, provides only standard user services, and supports up to 40 users per domain. Interconnects using X-Band SATCOM, digital line of sight, or military landline. The service includes non-CIS assets: tents, ECU, UPS, and generators to enable operation in harsh environments between -30° and +49° Celsius. This Service provisions the user equipment for 30 users that can be augmented by the DCEP Service (INF020) to bring it up to 40 users.

Afloat Command Platform (ACP) (PLT007) –a 3 domain system integrated into transit cases, meets the requirement for a Joint Task Force (JTF) deployed on-board a NATO flag ship in support of NRF or a Maritime heavy operation, can operate self-sustained without reach-back to the data centre, provides standard user services and capable of hosting a limited set of FAS applications, supports up to 110 users per domain. Interconnects using SATCOM provided by the hosting vessel. Dependent on the hosting vessel to provide 18 KW of electric power and sufficient cooling. Provisioned with the user equipment for 110 users.

Mini Point of Presence (Mini-PoP) (INF018) – a 2 domain system integrated into transit cases capable of supporting low intensity operations, dependent on reach-back to data centre for services, provides only standard user services, not NRF or FMN compliant, and supports up to 12 users per domain. Interconnects using X-Band SATCOM, digital line of sight, or military landline. The Service non-CIS support is limited to the UPS. The Service provisions the user equipment for 12 users that cannot be augmented.

Theatre Liaison Kit/ In-Theatre Liaison Kit (TLK/ILK) (INF019) – a 2 domain system integrated into transport cases capable of supporting low intensity operations, dependent on reach-back to data centre for services, cannot operate self-sustained, provides only standard user services, not NRF or FMN compliant. The system operates in one of three modes. BGAN, military SATCOM or terrestrial mode of operation. BGAN can operate up to 7 devices concurrently, which is a maximum of up to 3 laptops and 4 IP phones across the domains. The military SATCOM and terrestrial operation modes can operate up to 10 devices concurrently, which is a maximum of up to 6 laptops and 4 IP phones across the domains. The Service does not include any non-CIS assets. It provisions the user equipment for a maximum of 10 physical devices that cannot be augmented.

DCIS – Remote Network Module (RNM) (INF045)

The Remote Network Modules enable connection of nationally owned Deployable Communication and Information Systems (DCIS) to NATO DCIS in order to maintain and exercise Command and Control (C2) in accordance with the operational requirements of the NATO Readiness Forces (NRF). The users connected to the national DCIS will benefit from services hosted remotely on the NATO DCIS with neither DCIS system having to deploy. By adding a User Access Module (UAM), the RNM has the functionality to host up to 20 directly connected users per information security domain who will receive services provided from the remote NATO DPOP. This function does not require the connection of national DCIS system. The RNM can connect to the NATO DCIS described under INF035 (INF008 and INF009) in the NCI Agency Costed Customer Service Catalogue (CCSC). All services hosted on the NATO DCIS system are available for extension to and through the Remote Network Module.

Maritime Command and Control Platform (MAR C2P) Service (PLT012-1 and PLT012-2)

Former name of the service: SNFC2P

PLT012 Maritime C2 Platform (MAR C2P) service provides deployed C2 services designed to be installed on maritime vessels. There are 2 flavours of MAR C2P

PLT012-1 Single Domain MAR C2P Service provides a single domain deployable NATO instantiation of the Bi-Strategic Command Automated Information System (Bi-SC AIS) Communication and Information Systems (CIS), enabling delivery of bespoke maritime Command and Control (C2) services (as specified in the service agreement) for up to 20 users. The PLT012 service includes provision of remote support to the SNFC2P throughout its deployment and on board maintenance and support in exceptional circumstances. The PLT012 service requires connectivity through the existing CIS architecture of the hosting vessel, which is outside of scope of PLT012. Deployment of PLT012 onto a vessel, including coordination of connectivity, can separately be requested through ordering SME008 Maritime Operational CIS Deployment and Recovery Service.

PLT012-2 Dual Domain MAR C2P service (available from 2025) updates the single domain service, to provide maritime C2 services (as specified in the service agreement) in 2 security domains: up to 22 users in the classified domain; and up to 5 users in the unclassified domain. The PLT012-2 service connects through the operational anchor functions and the deployable gateway. The PLT012 service includes provision of remote support to the MAR C2P throughout its deployment and on board maintenance and support in exceptional circumstances. The PLT012 service requires connectivity through the existing CIS architecture of the hosting vessel, which is outside of scope of PLT012. Deployment of PLT012 onto a vessel, including coordination of connectivity, can separately be requested through ordering SME008 Maritime Operational CIS Deployment and Recovery Service

SEMARCIS/SEMARCOM Deployable Maritime CIS (INF044)

SEMARCOM provides single user secure access communication and information systems (CIS) as well as the corresponding services enabling deployed commands to exercise Command and Control (C2) between NATO and non-NATO Nation (NNN) vessels in a NATO Operation / Mission / Exercise. SEMARCOM provides a single user, single domain system integrated into transport cases capable of supporting low intensity operations. It supports the parallel use of Inmarsat FleetBroadband Streaming, IP background and PSTN calls (all 3 services concurrently). The Service is provided with Broadband Global Area Network (BGAN) satellite terminal. It provisions the user equipment for 1 user that cannot be augmented.
SEMARCIS provides increased functionality. SEMARCIS provides interoperability with SEMARCOM plus enhancements providing up to 2 users to include: An additional Ethernet switch and an additional backup Firewall at the NDOG to improve system continuity. SEMARCIS is capable of exchanging secure, mission critical information between the NATO Command platform and the maritime assets provided by Non-NATO Nations. A fall-back over BGAN to MARCOM will be configured to appropriate server in Jchat, web browser, or VoIP phone. The Service does not include any non-CIS assets. It provisions the user equipment for 2 users that cannot be augmented.

Features of flavours are provided in the table below.

Feature/Option	DragonFly	CGS	LINC-E	IMCD	ACP	RNM	Mini-PoP	TLK/ILK	SNF C2P	SEMARCOM / SEMARCIS
General										
Maintenance and repair of non-CIS equipment and supply of L1 – L3 system spare parts and consumables, including also crypto spares, is included within the funding specified in the service provisioning agreement.	X	X	X	X	X	X	X	X	X	X
Maintenance/ sustainment/ replacement of UPSs	X	X	X	X	X	X	X		X	
Included NCI Agency Services										
WPS001 Managed Devices Service - Laptop	X	X	X	X	X		X	X	X	
WPS009 Voice Collaboration Service	X	X	X	X	X		X	X		
WPS010 Video (VTC) Collaboration Service	X	X	X	X	X		X			
WPS012 E-Mail Service	X	X	X	X	X		X	X		
INF003 Enterprise Internet Access Service	X	X	X	X	X		X	X		
INF007 Infrastructure Storage Service	X	X	X	X	X					
WPS007 Print/ Scan/ Copy Service	X	X	X	X	X		X	X		
INF016 Infrastructure Backup/Archive Service	X	X	X		X					
INF001 LAN Service	X	X	X	X	X		X			
INF002 NATO General Purpose Communication System (NGCS) Point of Presence (PoP) Service (only WAN Infrastructure Assets feature)	X									
INF005 Infrastructure Integration Service	X	X	X	X	X		X			
PLT001 Information Sharing and Collaboration Platform Services	X	X	X	X	X					
PLT003 Web Hosting Service	X	X	X	X	X					
PLT006 Database Platform Service	X	X	X	X	X					
WPS014 Secure Voice Service	X	X	X	X	X		X			
APP029 Military Message Handling Application Service	X	X	X	X	X					
Included CIS Assets										
µCOM	X	X	X	X	X					
IEG-B and IEG-C	X	X	X		X					
Break Our Boxes (BOB)	X	X	X	X	X		X		X	
MS Core	X	X	X	X	X		X	X	X	
NU Core	X	X	X	X	X		X	X		
NS Core	X	X	X	X	X		X	X	X	X
SATCOM Modems					X					
SATCOM terminals (DART and BBSST or BGAN).							X	X		X
Crypto Assets	X	X	X	X	X		X	X		
Helpdesk Assets	X	X								
NAS	X	X	X		X					
µISM	X	X	X	X	X					
Intra Nodal Distribution System (INDS	X									
Service Access Points (SAP)										
Cyber Defense	X	X	X	X	X		X	X		
Element Network Manager (ENM)	X									
Integrated Network Management System (INMS)	X									
Interface to Nations Module (INM)	X									
Remote Network Module (RNM)	X	X	X	X	X					

Feature/Option	**DragonFly**	**CGS**	**LINC-E**	**IMCD**	**ACP**	**RNM**	**Mini-PoP**	**TLK/ILK**	**SNF C2P**	**SEMARCOM / SEMARCIS**
Included Non-CIS Assets										
Power Generator		X		X						
Environmental Control Unit	X	X	X	X						
Power Generator Set (PGS)			X*							
Cargo Transport Cases	X*	X*	X*	X*	X*	X*	X*	X*	X	X
Racks					X*					
Uninterrupted Power Supply (UPS)	X	X	X*	X**	X*	X	X	X	X	
Transit case	X	X	X	X	X	X	X			
Tent (with Furniture)	X	X	X	X						
Biological Chemical Tent and Filters	X									
Manual Handling Equipment	X									
Available Options										
Additional Baseline Changes	X	X	X	X	X	X	X	X	X	
Increase in Service Availability	X	X	X	X	X	X	X	X		
Change to Service Restoration Period	X	X	X	X	X	X	X	X		
Additional Domain Change							X		X	
Functional Area Services (FASs to be specified within the service provisioning agreement)	X	X	X						X	
ISO standard transportation containers	X		X							
Additional Prerequisites										
Operators and maintainers completed the Agency approved training.	X	X	X	X	X	X	X	X		
Customer ensures the provision of secure facility to enable operation	X	X	X	X		X	X	X	X	X
Domain Availability										
Single domain										X
2 Simultaneous Domains						X	X	X	X	
3 Simultaneous Domains	X	X	X	X	X	X				

***** Number of assets depending on the chosen options

****** Number of assets depending on the requested operational configuration

Available on:

NATO Unclassified
NATO Secret
Mission Secret

Service Prerequisites: In general, the Service requires Qualified Operators provided by the customer and are trained to the standard specified by the Agency. Specific prerequisites, where applicable, are specified in the Service Flavours section.

Standard Service Support Levels:

Service Availability Target: The service is costed with an availability target of 95% excluding scheduled downtime for maintenance. This is based on the assumption that the system may be in remote locations without local Agency support.

Service Restoration Period: The service is costed with a restoration of 80% of all incidents within 3 calendar weeks. This is based on the assumption that the system may be in remote locations without local Agency support.

Service Cost / Price: The unit of measure for each of the Service Flavours is Per System. Price details available in the Costed Customer Service Catalogue.

INF036 DCIS – Deployable SATCOM Service

Service ID: INF036

Service Name: DCIS – Deployable SATCOM Service

Portfolio Group: Infrastructure Services

Service Description: The Service provides a Deployable CIS to deployed commands of the NATO high readiness Response Force (NRF) enabling them to:

- Communicate between deployed NATO command units.
- Access the NATO strategic communications infrastructure and the Bilateral Strategic Command (Bi-SC) Automated Information Service (AIS).
- Communicate with mission partnering Nations and non-governmental organisations.

Value Proposition: The Service extends C2 ability worldwide, thus enabling Operational Commanders to execute Allied Operations and Missions worldwide.

- Modularity: Discrete elements may be combined as required for the deployment scenario and equipment can be interchanged or upgraded without having to replace large bespoke modules.
- Scalability: configurable from small C2 deployments through to a large deployment.
- Deployability: Deployable SATCOM is a solution for rail, sea, and tactical air transport. It may be fully operational in theatre within 72 hours of arrival on site, with a subset of priority services to be available within 48 hours. equipment is integrated into either ruggedized outdoor and indoor transit cases or in shelters that can be loaded onto military transportation vehicles.
- Sustainability: comprises Commercial off the Shelf (COTS) software that are interchangeable, upgradable, reconfigurable and replaceable.
- Interoperability: provides interoperability with NATO Headquarters (HQ), Nations forces, Governments and Non-Government Organisations through standards-based interfaces and conformance to the NATO Federated Mission Network Interoperability Profile.
- Service Management : The customer will have direct access to the Agency Service Management team throughout the period of delivery as described in the OTH004 Service description.
- Reporting: The customer is provided with access to the NCIA ITSM Toolset that enables monitoring of the service status and service availability. Additionally, the monthly service activity reports are provided.

Service Features:

The NCI Agency services in deployed environment:

- SATCOM (INF012);

- Managed Devices Service - Laptop (WPS001);

The above listed services correspond with standard NCI Agency services, as described in respective service definitions. However, due to deployable nature of the entire Deployable SATCOM Service, features of these services may differ from the standard ones, and standard flavours and service support levels may be not applicable. Where required, these differences are to be elaborated in detail within the respective service provisioning agreement. Delivery cost of these services differs from the standard service rates, and it is included within Deployable SATCOM Service delivery cost.

CIS Assets: listed for each specific flavour in the Service Flavours section.

Non-CIS Assets: listed for each specific flavour in the Service Flavours section.

Configuration Changes:

Major – Defined as a significant change to the service with the replacement of components that have reached end of life. The schedule of Major Changes is agreed by both Provider and Customer in advance and is managed and maintained by both parties. The new configuration will be made available to the customer.

Minor – Defined as low risk, continuous routine housekeeping such as minor software maintenance, security updates, and patches. Minor Changes are conducted continuously throughout the lifecycle of the Service, undertaken by the Provider without affecting operational availability.

Maintenance:

Defined and provided by the NCIA as Preventative Maintenance Inspections (PMI) and Corrective Maintenance Inspections (CMI) on all Service assets.

- PMI – The PMI to the Service are conducted at support Level 3 (L3), as a standard, along with configuration changes schedules taking into account manufacturer's instructions on maintenance, or otherwise defined technical maintenance standards;
- CMI – In the event of Service asset failure, Provider undertakes CMI at support Level 3 (L3) and in accordance with the Customers' requirements as described in the service provisioning agreement.

Maintenance includes regular sustainment of used applications and related licenses.

Shipment and transportation: Service assets will be provided at Customer's disposition at any of customer's permanent locations. Full shipping between the repair- and peacetime location is included.

Spare parts: Service includes required stock of support L1 and L2 spare parts, as specified in the service provisioning agreement. L1 and L2 spares are delivered to the Customer baselined at the factory state. Provider holds L1 and L2 spares needed for PMIs, CMIs, and uplifts. All L3 spares are held by Provider. Local users hold L1 and L2 spare parts in accordance with recommended spare part list provided in the specifications for each system. Local users are responsible to request replenishments trough Provider's Material Request Procedure.

Additional Options: Additional Baseline Changes, Increase in Service Availability, and Change to Service Restoration Period.

Costing of options is conducted on per request basis. Options are to be requested along with any possible additional requirements for Major Changes. Any in-year change of options shall be dealt with in accordance with procedures agreed within the service provisioning agreement.

Service Flavours:

TSGT (INF021) – the Generation 3 Transportable Satellite Ground Terminal (TSGT) and Upgraded generation 2 terminals (UTSGT) are vehicle mounted Satellite transmission systems that are designed for high capacity links utilizing the military X-Band space segment. Each terminal is capable of providing up to six 8-Mbit satellite bandwidth carriers. Both types of terminal have a 4.6 m antenna and redundant 750 W amplifiers, and the TSGT has additional functionality with an addition of a rapidly deployable 2.4 m pop-up antenna with redundant 250 W amplifiers enabling the terminal to establish simultaneous communications over two different satellites. Each terminal is operated by the deployed CIS crew and can be remotely managed by NCI Agency utilizing an out of band management system.

The systems can be interconnected over Fiber optic Ethernet to Dragonfly, CGS, LINC-E, IMCD, or Mini PoP flavours of DCIS Nodes Service. The service is provided with non-CIS assets enabling operation in harsh environments between -30° and +49° Celsius.

Available sub-flavours:

- **TSGT3G – T1 Variant:** may use optionally the 4.6 meter or the 2.4 meter pop-up antenna, Dual Satellite Operation. Maintenance includes the re-integration of NSPA-maintained PGS into SATCOM systems by NCIA;
- **TSGT3G – T2 Variant:** equipped with the 2.4 meter pop-up antenna single satellite operation. Maintenance includes the re-integration of NSPA-maintained PGS into SATCOM systems by NCIA;
- **Upgraded TSGT (UTSGT):** 4.6m antenna single satellite operation.

Included CIS Assets:

- Antenna ;
- Redundant Solid state power amplifier (SSPA)
- Redundant Low Noise Amplifiers (LNA)
- PSK & EMS modems (quantities can be defined by the customer)
- Management system enabling remote operation and service monitoring.
- I.P. Baseband module
- System Engineer PC/ Laptop.

Included non-CIS Assets:

- Power Generation System (PGS; UTSGT only);
- Antenna heaters
- 3rd Generation TSGT Generator;
- Antenna Trailer TSGT 2nd generation;
- Shelters with AIRCO System (ECU);
- UPS;
- BC Protection System.

Number of non-CIS assets depends on the specific configuration for each deployment.

DSGT (INF022) – the Deployable Satellite Ground Terminal (DSGT) is a modular terminal in transit cases that can be transported by light commercial vehicles, designed for medium capacity links utilizing the military X-Band space segment. Each terminal has a 2.4 m 200 W single amplifier that is capable of providing up to four carriers with a total throughput of up to 12Mbit. Each terminal is operated by the CIS crew deployed and there is currently no remote management capability. The system can be interconnected over Fiber optic Ethernet to Dragonfly, CGS, LINC-E, IMCD or Mini Pop flavours of DCIS nodes. The service non-cis support is limited to the UPS.

Available sub-flavours:

- **1st Generation DSGT**: consists of a 2.4 meter X-band antenna with a 125W power amplifier and a maximum duplex data link capacity of 4 Mbit/sec on global beam.
- **2nd Generation DSGT**: consists of a 2.4 meter X-band antenna and featuring an upgraded 200 watt power amplifier and a maximum duplex data link capacity of 8Mbit/sec on global beam

Included CIS Assets:

- 1st Generation Deployable Transportable Satellite Ground Terminal (1st Generation DSGT);
- 2nd Generation Deployable Transportable Satellite Ground Terminal (2nd Generation DSGT);
- System Engineer PC/Laptops.

Included non-CIS Assets: UPS and Transit Cases.

DART and FAST Small (INF032) – Dual Band Auto Pointing Rapidly Deployable Terminal (DART) and the Flexibly Assigned Satellite Terminal (FAST) are small modular terminals in hardened cases rapidly deployable and transportable in light commercial vehicles, designed for low capacity links utilising the military X-Band and commercial Ku Band space segment. Each terminal has approximately 1 metre to 1.3 metre, 50W to 125W single amplifier that is capable of providing a single carrier with a nominal throughput of up to 2 Mbit. The deployed CIS crew operates each terminal, with no remote management capability. The system can be interconnected over Fibre optic Ethernet to Mini-PoP or ILK/TLK flavours of Deployable CIS Nodes Service.

Available sub-flavours:

- **DART SATCOM**
- **FAST Small SATCOM**

Flavours differ only by equipment manufacturer, with no essential technical differences.

Included CIS Assets:

- Dual Band Auto Pointing Rapidly Deployable Terminal (DART);
- Flexibly Assigned Satellite Terminal (FAST);
- Antenna 1m - 1.3m;
- Antenna Tracking Controller;
- Ruggedized Laptop.

Included non-CIS Assets: UPS, Tent, Cargo Vehicle Rough Terrain (CVRT type SHERPA), Trailer, and PGS.

Available on:

NATO Unclassified
NATO Secret
Mission Secret

Service Prerequisites:

User provided Qualified Operators

Standard Service Support Levels:

Service Availability Target: In accordance with the stipulations of the service provisioning agreement and based on the Customer requirements.

Service Restoration Period: In accordance with the stipulations of the service provisioning agreement.

Available NCI Academy Training not covered by service cost:

A0045	NATO Ku-Band VSAT Operator

INF021:

A0043	NATO X-Band TSGT G3 Operator Level 1
A0047	NATO X-Band UTSGT Operator
A0052	NATO X-Band TSGT G3 Operator Level 2

INF022:

A0040	NATO X-Band DSGT Operator Level 1
A0041	NATO X-Band DSGT Operator Level 2
A0903	NATO CALI DSGT Operator

INF032:

A0051	NATO DART+ Operator
Ref is TBC	FAST Small Operator

Service Cost / Price: The unit of measure for the Service is Per System. Price details available in the Service Rates document.

INF037 DCIS – Deployable Radio Transmission Service

Service ID: INF037

Service Name: DCIS – Deployable Radio Transmission Service

Portfolio Group: Infrastructure Services

Service Description: The Service provides a directional transmission service and secure voice and data transfer capability based on the HF/VHF radio communication systems to deployed commands of the NATO high readiness Response Force (NRF) enabling them to communicate between deployed NATO command units and down to the tactical user.

Value Proposition:

Transportable via road, rail, sea, and tactical air transport, the systems may be operational in theatre within 4 hours of arrival on site. The customer is provided with access to the NCIA ITSM Toolset that enables monitoring of the service status and service availability.

Service Management : The customer will have direct access to the Agency Service Management team throughout the period of delivery as described in the OTH004 Service description.

Service Features:

Included NCI Agency Services: listed for each specific flavour in the Service Flavour section.

Included NCI Agency Services correspond with standard NCI Agency services, as described in respective service definitions. However, due to deployable nature of the entire Deployable Radio Communications Service, features of these services may differ from the standard ones, and standard flavours and service support levels may be not applicable. Where required, these differences are to be elaborated in detail within the respective service provisioning agreement. Delivery cost of these services differs from the standard service rates, and it is entirely included within the Deployable Radio Transmission Service delivery cost.

Included CIS Assets: listed for each specific flavour in the Service Flavour section.

Included Non-CIS Assets: listed for each specific flavour in the Service Flavour section.

Reporting: Manually generated, no 24/7 monitoring of the Service status/availability feasible.

Configuration Changes:

Major – Defined as a significant change to the service, such as complete re-configuration of all or majority of key configuration items (change of the service baseline), primarily in order to prepare a service for a new mission.

Minor – Defined as low risk, continuous routine housekeeping such as minor software maintenance, security updates, and patches. Minor Changes are conducted continuously throughout the lifecycle of the Service, undertaken by the Provider without affecting operational availability.

Maintenance:

Preventative Maintenance Inspections (PMI) – The PMI to the Service are conducted at support Level 3 (L3) and in coordination with Customer to take into account the impact on operational availability and requirements, as a standard, along with configuration changes schedules taking into account manufacturer's instructions on maintenance, or otherwise defined technical maintenance standards;

Corrective Maintenance Inspections (CMI) – CMI is undertaken by Provider at support Level 3 (L3) in the event of Service asset failure, in accordance with the Customers' requirements as described in the service provisioning agreement. This includes replacement of non-reparable equipment, where applicable under NATO financial rules and regulations.

Shipment and transportation: Service assets will be provided at Customer's disposition at any of customer's permanent locations. Full shipping between the repair- and peacetime location is included.

Documentation: Customer will be provided with required technical documentation, as specified in the service provisioning agreement.

Spare parts: Service includes required stock of support L1 and L2 spare parts, as specified in the service provisioning agreement. L1 and L2 spares are delivered to the Customer baselined at the factory state. Provider holds L1 and L2 spares needed for PMIs, CMIs, and uplifts. All L3 spares are held by Provider. Local users hold L1 and L2 spare parts in accordance with recommended spare part list provided in the specifications for each system. Local users are responsible to request replenishments trough Provider's Material Request Procedure.

Security Accreditation Documentation: Customer will receive prepared documentation required for the Security Accreditation.

Additional Options: Additional Baseline Changes, Increase in Service Availability, Change to Service Restoration Period.

Customer requests for in-year Major Changes, in addition to the service provisioning agreement agreed Major Changes, shall be dealt with in accordance with procedures agreed within the service provisioning agreement.

Service Flavours:

DCIS HF (INF024-1) – the deployable High Frequency Radio system enabling secure voice and data chat services between the users in the field and the commands in the 3 – 30MHz range. The system is built into transit cases (t-cases) that can be deployed in a tent or building of opportunity. No interconnection to DCIS Nodes available.

Included CIS Assets: HF Radio Systems; with telescopic Clark mast and antenna and user laptop.

Included non-CIS Assets: Transit case.

DCIS HF (INF024-2) – the deployable High Frequency Radio system enabling secure voice and data chat services between the users in the field and the commands in the 3 – 30MHz range. The system is built into transit cases that can be operated from within the transportation vehicle or deployed in a tent or building of opportunity. No interconnection to DCIS Nodes available. The service includes supporting non-CIS assets to enable operation in harsh environments between -30° and +49° Celsius.

Included CIS Assets: HF Radio Systems; with telescopic Clark mast and antenna and user laptop.

Included non-CIS Assets: Biological - Chemical (BC) Shelter; Uninterruptible Power Supply (UPS); Power Assembly; Generators; Lifting Device.

Maintenance includes the re-integration of NSPA-maintained PGS into SATCOM systems by NCIA.

DLOS (INF025) – the deployable Line Of Sight is capable of establishing a Digital Transmission link utilising I.P. over Ethernet at a data rate of up to 800Mbit per second using adaptive modulation up to a distance of 50km. The system is assembled into transit cases operable from within the transportation vehicle or deployed in a tent or building of opportunity. Possible interconnection over Fibre optic Ethernet to INF035 Services. Non-CIS assets included to enable operation in harsh environments between -30° and +49° Celsius. Each system consists of one BC protected shelter mounted on an all-terrain vehicle.

Included CIS Assets: UHF Radio, Fibre Optic System; Switch; Modem; F.O. Multiplexer; Mast; Self-Aligning Antenna.

Included non-CIS Assets: BC-Shelter; ECU; UPS; Lifting device.

Available on: N/A

Service Prerequisites:

User provided Qualified Operators

Standard Service Support Levels:

Service Availability Target: In accordance with the stipulations of the service provisioning agreement and based on the Customer requirements.

Service Restoration Period: In accordance with the stipulations of the service provisioning agreement.

NCIA academy Trainings Available (INF025):

A00246	DLOS Operator/Technician

Service Cost / Price: The unit of measure for the Service is Per System. Price details available in the Service Rates Document.

INF038 DCIS – Deployable Nodes Anchor Service

Service ID: INF038

Service Name: DCIS – Deployable Nodes Anchor Service (Mission Anchor Function – MAF)

Portfolio Group: Infrastructure Services

Service Description: The Service enables the operational user to prepare the Deployable CIS Nodes in garrison and keep them at high readiness to deploy, as well as to interconnect to NATO General-Purpose Communications System (NGCS) when deployed. With the DCIS Nodes installed in garrison in the Mission Preparation Centre (MPC; a.k.a. PoP Replication Centre, PRC), they are interconnected to the Deployable Operational Gateway (DOG) from where they will synchronize the services, replicate all user data, and interconnect to deployed DCIS Nodes.[1]

Value Proposition:

The service enables the interconnection of INF035 services whilst in peace time location to any one of the prepared Mission Domains 24/7/365. The service enables the continuous replication of mission data and implementation of regular patch updates thus ensuring that the DCIS systems are ready to deploy at very short notice.

The customer will have direct access to the Agency Service Management team for Deployable CIS and will be supported as described in the OTH004 Service Description.

The Service includes sufficient tools and test equipment to prepare the DCIS Nodes, Satellite Communication, and Radio Transmission assets for deployment and subsequent interconnection to NGCS.

Service Features:

Included NCI Agency Services: listed for each specific flavour in the Service Flavour section.

Included NCI Agency Services correspond with standard NCI Agency services, as described in respective service definitions. However, due to deployable nature of the entire Deployable Nodes Anchor Service, features of these services may differ from the standard ones, and standard flavours and service support levels may be not applicable. Where required, these differences are to be elaborated in detail within the respective service provisioning agreement. Delivery cost of these services differs from the standard service rates, and it is entirely included within the Deployable Nodes Anchor Service delivery cost.

[1] Throughout this Service Description, all reference to Mission Secret (MS) network or domain is to be considered under the new Vigilance and Enhanced Vigilance Activities Mission Network (VeVA MN) SH/CYBER/J6/SPP/080/23-015016 – Implementation of VeVA MN – dated 16 Oct 2023

Included CIS Assets: listed for each specific flavour in the Service Flavour section.

Included Non-CIS Assets: listed for each specific flavour in the Service Flavour section.

Reporting: This service is monitored 24/7 and availability reports will be provided.

Configuration Changes:

Major – Defined as a significant change to the service, such as complete re-configuration of all or majority of key configuration items (change of the service baseline), primarily in order to prepare a service for a new mission.

Minor – Defined as low risk, continuous routine housekeeping such as minor software maintenance, security updates, and patches. Minor Changes are conducted continuously throughout the lifecycle of the Service, undertaken by the Provider without affecting operational availability.

Maintenance:

Preventative Maintenance Inspections (PMI) – The PMI to the Service are conducted in coordination with Customer to take into account the impact on operational availability and requirements, as a standard, along with configuration changes schedules taking into account manufacturer's instructions on maintenance, or otherwise defined technical maintenance standards;

Corrective Maintenance Inspections (CMI) – CMI is undertaken by Provider in the event of Service asset failure, in accordance with the Customers' requirements as described in the service provisioning agreement. This includes replacement of non-reparable Besides PMI and CMI at Level 3 of the MPC network and information system hardware, the Service includes shipping (3 locations) to/from repair facility, and supply of Level 1 through Level 3 system spare parts and consumables. In support of the DCIS mission preparation, the Provider conducts overall management of all activities.

Additional options: Additional Baseline Changes; Increase in Service Availability; Change to Service Restoration Period.

Service Flavours:

DOG (INF026) – the Deployable Operational Gateway Service (DOG) provides two anchor points for all NATO deployable forces that interface into the NATO General Purpose Communication Systems (NGCS) static CIS network as well as between NATO Secret (NS) and Mission Secret (MS) domains, or among different MS domains. Each of the DOG systems provides 4 (four) security domains (NS, NU, and 2X MS), with each domain providing the complete set of mission information exchange requirements to support the operational commands on deployment. The DOG is hosted in the two NCI Agency data centres and are interconnected with the Satellite Ground Stations (SGS) and Mission Information Room (MIR) that enables enterprise wide connectivity of users to the mission services.

Included NCI Agency services: LAN Service (INF001); NATO General Purpose Communication System (NGCS) Point of Presence (PoP) Service (INF002); Enterprise Internet Access Service (INF003); Infrastructure Integration Service (INF005);

Infrastructure Storage Service (INF007); Infrastructure Backup/Archive Service (INF016); Managed Devices Service for the system administrators (WPS001); E-Mail Service (WPS012); Print/ Scan/ Copy Service (WPS007); Voice Collaboration Service (WPS009); and Video (VTC) Collaboration Service (WPS010).

Maintenance is conducted at support Levels 1-3 (L1-L3), and it includes regular sustainment of used applications and related licenses.

Configuration and maintenance of the backup capability is included.

Available sub-flavours:

- None

Included CIS Elements:

- Terrestrial network connectivity into NGCS and the respective NS, MS and NU domains;
- Satellite Connectivity;
- BGAN network interconnectivity with Inmarsat (NDOG);
- X Band Satellite connectivity through the SGT terminal (MDOG) with each MDOG able to provide connectivity for 12 deployed TSGTs;
- An IEG-C for cross-domain service flows;
- Cross-domain Service interfaces for Mail, Voice and VTC.

Included CIS Assets:

- Transmission and Network layer routing with redundancy;
- Distribution Layer Switches;
- Border Protection Firewalls;
- Voice Call Managers;
- VTC Conference units;
- Cross domain capability for mail and file transfers, low to high and between high side domains;
- Centralised Services for security patching for each domain;
- Crypto Equipment.

MPC/PRC (INF027) – the Mission Preparation Centre or PoP Replication Centre (MPC or PRC) is an in-garrison capability to connect Deployable Nodes in the static domain to the deployed Mission Secret domains in order to enable the replication of user data and the update of services between the DOG and Deployable Nodes. The MPC/PRC capability is essential to support the operational requirement for 48 hours or 5-days notice to move. For MPC/PRC on short NTM, e.g. assigned to mission in stand-by, COI enabling and COI services are installed and operational, supporting the generic C2 service requirements of the JTF or LCC HQ that the specific PoP will support upon deployment. Additionally, all applicable IA tools and processes are set as active. In support of the DCIS mission preparation, the Provider conducts overall management of all services, to include enabling the distribution of Mission-specific configuration updates, system patches, security patches and updates, and also supports on-the-job training of Customer personnel.

Included NCI Agency services: Gateway Security Service (SEC011); Managed Device Service (WPS001); and Print/ Scan/ Copy Service (WPS007).

Maintenance is conducted at support Level 3 (L3).

Spare parts: This flavour of the Service includes required stock of support L1 and L2 spare parts, as specified in the service provisioning agreement. L1 and L2 spares are delivered to the Customer baselined at the factory state. Provider holds L1 and L2 spares needed for PMIs, CMIs, and uplifts. All L3 spares are held by Provider. Local users hold L1 and L2 spare parts in accordance with recommended spare part list provided in the specifications for each system. Local users are responsible to request replenishments trough Provider's Material Request Procedure.

Included CIS Assets: Server Hardware.

Prerequisite: INF038 DCIS – Deployable Nodes Anchor Service (DOG flavour). Locations hosting systems require appropriate security certification for storage and use of cryptographic equipment and key material, connection to the NGCS Protected Core Segment which allows interconnection with the NGCS Gateways, deployed nodes and the NCI Agency Network Control Centre (within ESOC), and sufficient test equipment to simulate other Nations' networks.

Available on:

NATO Unclassified Domain
NATO Secret Domain
Multiple Mission Secret Domains

Service Prerequisites: None, unless specified in the Service Flavours section for specific flavours.

Standard Service Support Levels:

Service Availability Target: In accordance with the stipulations of the service provisioning agreement and based on the Customer requirements.

Service Restoration Period: In accordance with the stipulations of the service provisioning agreement.

Service Cost / Price: The unit of measure for the Service is Per System. Price details available in the Service Rates document.

INF039 E-Mail Federation Service

Service Retired and became a flavour under WPS002 - Enterprise Identity Access Management Service (Former User Access Service).

INF040 Ultra High Frequency (UHF) Tactical Satellite (TACSAT) Radio Services

Service ID: INF040

Service Name: UHF TACSAT Services

Portfolio Group: Infrastructure Services

Service Description: The NATO Ultra High Frequency (UHF) Tactical Satellite (TACSAT) Radio Services provide secure low data rate communication links to the tactical edge in all battle-space environments, in both the back-pack and vehicle-mounted configuration.

The TACSAT terminals come equipped with a U.S Type 1 Control Cryptographic Item (CCI) radio and associated ancillaries required to communicate in both secure voice and secure data at all NATO classifications. The NATO terminals are capable of operating in Single Carrier Per Channel (SCPC), Demand Assigned Multiple Access (DAMA) and Integrated Waveform (IW), with data rates of up to 64Kb/s.

The current NATO TACSAT is the Harris AN/PRC 117F.

Please note that this service does not cover the TACSAT network subsystem, the NATO UHF Control Capability (NUCC); this is covered under the INF012 SATCOM Service.

The customer will have direct access to the Agency Service Management team for Deployable CIS and will be supported as described in the OTH004 Service Description.

Value Proposition: NATO's UHF network is a set of complex systems that provides NATO forces with access to a secure tactical radio SATCOM network across NATO's Area of Responsibility (AOR). The UHF SATCOM capabilities are used to support NATO Land, Sea and Air operations, providing secure voice and data capabilities.

The UHF TACSAT network and terminal requirements are based on the need to support the Core mission requirements associated with Capability Level 1 and 2, which represent the MJO 1, SJO 2, SJO 5 and SJO 6 missions. In addition, any Allied Operations and Missions (AOM), standing air and maritime requirements as well as training requirements have been taken into consideration.

Service Features: Point to Point and Point to Multi Point Tactical communications consisting of voice, email, chat and local FTP.

Service Request: The ACO-endorsed technical report 2017/NSP011502/01 defines the quantity and allocation plan of the current and future NATO TACSAT terminals. Requests for TACSAT assets outside of the technical report must be pre-approved by ACO J6 via formal communication before the assets will be released by NCIA through ITSM and EBA.

Service Flavours: The UHF TACSAT Radios capability consist of two variants:

- On-The-Pause (OTP), back-pack portable configuration and On-The-Move (OTM), vehicle- or mobile-mounted configuration
- Static installation, consisting of the additional equipment (Matrix switch, antennas, amplifiers, cables etc) installed at static sites

Available on:

Standalone

Service Prerequisites:

To be able to utilise the TACSAT SATCOM service a Satellite Access Authorisation (SAA) must be in place through the SATCOM Service (INF012).

Standard Service Support Levels*:*

Service Availability Target: 95.0 %

Service Restoration:

	Restoration Time
Level 0 Related (User)	<2 hrs
Level 1 Related (CSU)	2-24 hrs
Level 2 Related (CSSC)	1-10 working days
Level 3 Related (Vendor)	>90 working days

Available NCI Academy Training not covered by service cost:

A0037	UHF TACSAT Basic
A0038	UHF TACSAT Applications & Data Base Manager

Service Cost / Price: The unit of measure for the Service is Per Device. For price details please see the Service Rates Document.

INF041 CRC System Interface (CSI) Local Support Service

This service is moved under the APP087 CRC System Interface (CSI) Application Service as one of its service flavours. The service ID INF041 will be retained for financial tracking purposes (please see APP087 for further clarification).

INF042 ADatP-3 Gateway Service

Service ID: INF042

Service Name: ADatP-3 Gateway Service

Portfolio Group: Application Services

Service Description: Currently NATO CAOCs use ICC as their primary Air C2 system while subordinate ARS are gradually moving to ACCS. This requires exchange of message-based information products, ADatP-3, between ACCS and ICC. ACCS uses STANAG 4406 as messaging protocol while ICC uses SMTP. This requires translation between STANAG 4406 and SMTP messaging protocols, which is provided by the ACCS AdatP-3 Gateway (GWY).

Value proposition: The service enables the exchange of formatted (AdatP-3 messages) between ACCS and ICC.

Service Features: The ACCS SMTP gateway consists of two COTS products, XOMail server for STANAG 4406 and Exchange server for SMTP translation. The GWY is currently available and working but it is considered as a single point of failure for its centralized architecture

Service Flavours:

None

Available on:

NATO Secret

NATO Classified

Service prerequisites:

APP049 (ICC)

APP050 (ACCS)

SEC022 (ALF-SFP)

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

Monday to Thursday: 0600 to 2200 (CET)
Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number:

Belgium +32 65 44 3177
Netherlands +31 70 374 3177
Italy +39 081 721 3177
Germany +49 282 4978 3177
USA +1 757 747 3177
For NATO HQ +32 02 707 5858

Service Requests:

To request the INF042 service please complete the Customer Request Form and contact NCI Agency Demand Management. https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions between NCIA and SHAPE on an annual basis via AMDC2 ISS POW.

Service ID	Service Name	Service Flavour/Option	Service Unit of Measure
INF042A	ADatP-3 and Air Traffic Management (ATM) Gateway Service	AdatP-3 Gateway	1
INF042B	ADatP-3 and Air Traffic Management (ATM) Gateway Service	ATM Gateway	1

KPIs: No service availability monitoring KPIs are defined.
In case an SLA is established for AdatP-3 Gateway support the standard NCI Agency service support KPIs (response and restoration times) apply unless otherwise negotiated.

INF043 NATO Partner Network Service

Service ID: INF043

Service Name: NATO Partner Network Service

Portfolio Group: Infrastructure Services

Service Description: The NATO Partner Network Service provides Secured NATO client devices that allow collaboration among NATO and Military Partnerships entities to cooperate and share documentation up to a Security level of NATO Unclassified.

The Client device is loaded with the office automation software (MS Office Professional Suite and Adobe Acrobat Reader), Windows operating system, and NATO recommended security tools.

The service can also provide Remote connectivity via NATO Enterprise Managed Mobility Service.

Value proposition: The NATO Partner Network Service is a bundle of customer facing services (Managed Device, Enterprise Identity Access Management Service, E-mail Service, Printer Service and Information sharing and collaboration Platform Service, Infrastructure and Security Services). This allows the production of documentation, presentations etc., in support to the business processes of the NPN users located in SHAPE campus; the service also allows collaboration with external entities via email capability and can be extended to external entities via Remote connectivity capabilities.

Service Features: The Service includes a fully NATO managed end user device and a possibility to collaborate within the NPN Domain via a customized Web Content Management Portal. The NPN Partner Network Collaboration Service also includes an E-Mail capability.

Service Flavours:

Portable Client Device (Laptop) – provides a Laptop device that needs to be connected to a wired or wireless network. A power supply and an external mouse are also included in the package. Access to the NPN network is provided via a secure VPN solution.

Static Solution – provides a laptop device connected to an internal wired network. This solution features a docking station, a media converter, an external monitor, a keyboard, and a mouse.

Available on:

NATO Partner Network Unclassified

Service prerequisites:

This service encompasses a number of other catalogues services (INF, PLT, WPS, SEC).

Standard Service support levels:

Service Availability Target: 99.0% Availability

Service Restoration: The service delivered as P4.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the service is 1. The total of the service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

Please see Service Delivery Lifecycle Stages section for more information about the general overview of the type of deliverables involved in each stage and the scope of corresponding service rate.

Please see Service Rates document for standard rates applicable to the service.

INF044 SEMARCIS/SEMARCOM Deployable Maritime CIS

This service is moved to INF035 DCIS - Deployable Nodes Service as of CCSC v9.0 as a flavour.

INF045 DCIS Remote Network Module (RNM)

This service is moved to INF035 DCIS - Deployable Nodes Service as of CCSC v9.0 as a flavour.

INF046 Naming and Registry Authority (NRA) – IPv6 Local Internet Registry (LIR) Service

Service ID: INF046

Service Name: Naming and Registry Authority (NRA) – IPv6 Local Internet Registry (LIR) Service

Portfolio Group: Infrastructure Services

Service Description: NRA IPv6 LIR service looks forward to IPv6 with an aim to enable nations to have their own block of address space. The NCI Agency Naming and Registration Authority (NRA) is a registered LIR (Local Internet Registry) thus able to sponsor and 'resell' IP address space, the INF046-D service flavour provides a cost centre addressable to the Nations for procurement and ongoing administration of IPv6 addresses. In this service offering the NRA will procure, administer and protect the address allocation with the relevant Regional Internet Registry, the requirement for management of the address space within the nation network remains with the nation, where NRA will offer consultation via INF046-C.

Value proposition: This service provides value to customers through the collation and sharing of centrally registered items Alliance-wide, improving data integration, assuring global uniqueness, and protection from collisions in names, numbers and semantics. As organizations become data-enabled, simultaneous with an accelerating data velocity, the criticality of master data management has grown to be an imperative.
IPv4 address has all but run out, few nations are fortunate enough to already possess their own block of IP address. For the Service flavour, IP Sponsoring LIR (Local Internet Registry) NRA will act as a Sponsoring LIR for a NATO nation wishing to procure IPv6 address space for national, NATO secret, mission or AFS use. Further NRA will consult and advise on best application of this new technology within the Nation or entity.

Service Features: This service offering provides Nations and NATO affiliated entities the capability to procure their own IPv6 address space through NATO. This will in the future be a key enabler on both the NU (Internet) and MS/NS networks under both FMN and AFS. Further providing consultancy service to support the deployment and roll out of IPv6 technology.

Service Flavours: NRA offers different flavours according to different data spheres

> **INF046-C IPv6 Consultation:** Consultation enables advice and registration on the usage, deployment and transition to IPv6. One time consultation is a prerequisite for IN046-D. Included in this cost is the consultation on super-net addressing plan following AFS principals (nation manages addressing). Further Consultation may be purchased provided per Subnet Allocation.
>
> **INF046-D IPv6 Sponsoring LIR NRA**: Sponsorship enables a nation (or entity) to receive a single allocation of IPv6 address space. This is an annual reoccurring service for maintenance and sponsorship of IPv6 address space, instantiation of this flavour requires consultation (INF046-C) for the super-net allocation.

Available on:

All Networks

Service Prerequisites: NATO member, NS nation connection is behind a NNG (AFS) or for a none-NATO nation, the MS connection is behind a NIP (FMN)]

Standard Service Support Levels*:* **[***N/A or specific statement if below lines are not applicable to the service, e.g. if the service is a SME-based one***]**

Service Availability[1] Target: [*During heavy load times BAU requests will receive lower priority than mission critical warfighting requests. Registration and allocation services work on a 2 week (10 working day) delivery window, however this may be further delayed if provided information is not thorough and correct. This delivery window is to facilitate clarifications, ensuring forward planning and data integrity; once registration and allocation are complete, a new ticket must be raised for changes and amendments not in the original ticket.***]**

Service Restoration: [*For service degradation NRA will act (MTTR) within 1 working day of an incident notification, NB in some instances full restoration will be beholden to the vendor timelines and availability.*

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. **]**

Service Cost / Price: INF046-C flavour is costed per allocation per Security domain. INF046-D is costed per allocation (recommended each nation 1x allocation). Ongoing annual service will cover administration, de-confliction, cessation, maintenance, monitoring and reporting.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

INF048 Data Science Infrastructure as a Service

Service ID: INF048

Service Name: Data Science Infrastructure as a Service

Portfolio Group: Infrastructure Services

Service Description: Data Science Infrastructure as a Service (DS-IaaS) provides access to the computing and storage infrastructure typically needed for performing computationally intensive machine learning activities, together with the high capacity, fast storage needed for machine learning from large data sets or for big data analysis.

Value proposition: The Service offers the following benefits:

- Increased speed for machine learning and big data analysis functions, due to specialised processors and storage.
- Increased productivity of AI development and other data science activities.

Service Features: Data Science Infrastructure as a Service offers the user the following features:

- Combined high-performance compute and storage capacity;
- Lifecycle management of the computing environment;
- Software licensing and maintenance e.g. GPU and CPU virtualisation;
- Capacity provisioning through scalable and flexible management of available resources;
- NATO accredited environments for secure handling classified data.

Service Flavours: There is a single flavour for this service:

- Custom sized virtual hardware on NATO SECRET on-premise computing platform.

Available on:

NATO SECRET, classification up to including NS

Service Prerequisites:

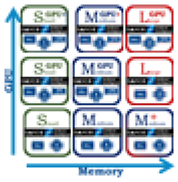
WPS001 for NS services.

Service Availability Target : 98%

Service Restoration Priority : P3

N.B. This service is not intended to support operational or business users directly.

Service Cost / Price: The unit of measure for the service is IaaS unit. There is a mandatory monthly fee per named user (Advanced IaaS user profile) . User profile required to work on virtual machines (IaaS or PaaS) on NATO SECRET Data Science Infrastructure. There is a mandatory monthly fees per named user (Advanced PaaS user profile).User profile required for those working on virtual machines (IaaS or PaaS) on NATO SECRET Data Science Infrastructure.

Infra	Description	IaaS Units
	Custom sized virtual hardware	Per unit: • 8 vCPU • 64 GB RAM • 8GB vGPU A multiple of units can be requested.

INF049 Air Traffic Management (ATM) Gateway (GW) Service

Service ID: INF049

Service Name: ATM Gateway Service

Portfolio Group: Application Services

Service Description: The ATM GW is a system that feeds any AirC2 system, with the flight plans provided by the various national Air Traffic Control (ATC) systems. This function is fundamental in order to create a credible and complete Recognised Air Picture (RAP) in the various ARSs where it is installed because it facilitates the correlation/recognition of the Air Breathing Threats (ABTs)

Value proposition: The service enables the exchange of flight plans and ATM Data between AirC2 systems and ATM/ ATC Centres.

Service Features: The ATMGW consists of a redundant HW server, operating a Linux OS, with an ATMGW Server and Client to receive and transmit Flightplan messages in different message formats (ICAO and ADEXP), to convert those messages in a different format and to receive and transmit these messages via different protocols (AFTN, AMHS, FMTP, FDE)

Service Flavours: The ATMGW Server/client configuration represent a singleton service in support of active ACCS sites

Available on:

NATO Secret

NATO Classified

Service prerequisites:

APP050 (ACCS) – (or non-ACCS system i.e. MASE)

SEC022 (ALF-SFP)

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

Monday to Thursday: 0600 to 2200 (CET)
Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number:

Belgium +32 65 44 3177
Netherlands +31 70 374 3177
Italy +39 081 721 3177
Germany +49 282 4978 3177
USA +1 757 747 3177
For NATO HQ +32 (0)2 707 5858

Service Requests:

To request the INF049 service please complete the Customer Request Form and contact NCI Agency Demand Management. https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions between NCIA and SHAPE on an annual basis via AMDC2 ISS POW.

Service ID	Service Name	Service Flavour/Option	Service Unit of Measure
INF049	ADatP-3 and Air Traffic Management (ATM) Gateway Service	ATM Gateway	1

KPIs: No service availability monitoring KPIs are defined.
In case an SLA is established for ATM Gateway support the standard NCI Agency service support KPIs (response and restoration times) apply unless otherwise negotiated.

NATO Communications and Information Agency

INF053 Internet Website Publishing and Protection Service

Service ID: INF053

Service Name: Internet Website Publishing and Protection Service

Portfolio Group: Infrastructure Services

Service Description: The Internet Website Publishing and Protection Service provides the cradle to grave management of the publication of NATO websites on the Internet. This includes the coordination required for the site to abide by the applicable NATO Security Directives, the issuing of NATO.INT DNS names, the provision of required SSL certificates, the annual revalidation of the site, and eventual decommissioning of the site.

The service will additionally provide the health monitoring for all Websites covered by this service to fast response

Value Proposition: Internet Website Publishing and Protection Service adds value to NATO through the central oversight of the process to publish NATO.INT and NATO affiliated websites to the Internet. This oversight adds value through the application of NATO Web Application Security Directive, secure public certificate issuance and continual site attribution.

Service Features:

- NATO Security Directive Coordination
- Web Application Security Remediation Coordination
- NATO.INT Internet DNS Publication
- Public PKI Certificate Issuance
- Content Delivery Network (CDN)
- Denial of Service Protection
- Continuous Site Oversight
- Website Decommissioning

Service Flavours: The service is in support of the Web Governance Directive and applies to each site requested to be publicly accessible over the Internet with NATO.INT domain name. Additional NATO affiliated sites may also subscribe to this service.

- **INF053-1 Standard:** The standard service flavour is for average website with expected average activity. This will provide the coordination activities required to publish the site on the Internet, two public PKI certificates (CDN edge and the origin server), cloud based content delivery network coverage, denial of service protection, revalidation of website with site owners and eventual decommissioning of the website.
- **INF053-2 Flagship:** The flagship service flavour is for NATO Flagship websites with expected heavy activity. This will provide the coordination activities required to publish the site on the Internet, two public PKI certificates (CDN edge and the origin server), cloud based content delivery network coverage, denial of service protection,

revalidation of website with site owners and eventual decommissioning of the website.

Available on:

Internet

Service Prerequisites:

None

Standard Service Support Level: N/A

Service Cost / Price: The unit of measure is per site (URL).

This page is left blank intentionally

Platform Services

This page is left blank intentionally

PLT001 Information Sharing and Collaboration Platform Services

Service ID: PLT001

Service Name: Information Sharing and Collaboration Platform Services

Portfolio Group: Platform Services

Service Description: The Service provides a platform for NATO entities to create, collaborate and share information internally within the Alliance and/or externally between NATO and External Partners. The Service provides a secure, online portal/website for users to create, capture, store, manage, broadcast, publish, view, and search all types of digital content. It allows organizational elements to establish a rich collaboration environment by utilising and combining web information publishing and portal feature options. The Service enables collaboration and social capabilities in the context of team, community, NATO Enterprise, NATO Nations, PfP Nations, Industry, and Academia.

Value Proposition: The Service provides a comprehensive collaboration experience, with rich interaction through calendars, lists, libraries, blogs, wikis, etc. thus the Service allows users to work together effectively by sharing information and jointly working on documents. The offered collaboration and social services are an enabler for an effective Information and Knowledge Management (IKM) within a controlled information lifecycle, in compliance with NATO IM Policies, and protected.

Service Features: The Service provides the following features (subject to the specific Service Flavours):

1. Content Management:
    - Sites is where all collaboration happens. Sites contain many features, including the capability to create, store, and retrieve data, and manage, tag and search for content and information.
2. Document Management:
    - Allows document collaboration with rich document experience on co-authoring, version control and secure sharing.
    - Connectivity with Microsoft Office client applications through lists and document libraries.
    - Apps for SharePoint, workflows, Word or Excel Services.
3. Social:
    - Provides social networking capabilities, newsfeeds, and profile searching and tagging, along with the capability to search, locate and interact with people through their skills, organizational location, relationships.
    - Blogs, wikis, surveys, metadata tags and other.
4. Search: the ability to search content from multiple sources, fine-tuned with facets, filters and autocomplete.
5. Staging environment to assist with capturing customer functional requirements or executing User Acceptance Tests (available on request).

Service Flavours: The Service is available in four flavours:

NATO Enterprise Collaboration Platform: A site with a dedicated URL address based on the “NATO Enterprise Portal Templates” as building blocks, enabling customers to manage and design the site by combining available building blocks (Landing, Exercise, Document Collaboration, Project, Events and more). These templates provide the NATO Visual Identity, a set of NATO purposed web parts and standard document metadata compliant with the “NATO Core Metadata Specification” (NCMS), easing the learning curve and fostering its usability. They can scale up to the full storage limit of SharePoint, requires no downtime for updates and are responsive (available for mobiles and tablets). Default storage size is 10 GB [1].

Best for: customers who require sites with publishing or/and collaboration features with a high degree of autonomy for designing and content authoring while aligning with the NATO metadata and look and feel standards.

Customer-specific SharePoint Collaboration Platform: A site with a dedicated URL address and selected SharePoint features specifically tailored to customer requirements. Default storage size is 10 GB [2].

Best for: customers who require a standard SharePoint “out of the box” implementation in combination with specific functionalities not available in the “out of the box” SharePoint offering, such as custom metadata, custom look and feel and content management features, or that require sophisticated workflows, fine-tuned security (by user, documents or shared spaces) or integration with other applications.

Communities of Interests (COI) Collaboration Platform: Quick delivery[3] Information management site that addresses the need for enhanced collaboration within and between NATO Communities of Interests (e.g. Electronic Warfare, Space, Cyber Security, CIS, Exercises and more). Information architecture and tools have been designed to strengthen teamwork within the subject-focused collaboration sites and enable exchange of information between different communities.
COI is accessible to NATO and Non-NATO entities, including Nations, Industry and Academia to support cooperation between NATO Enterprise and its External Partners. COI-templated sites follow the predefined NATO Visual Identity and are compliant with “NATO Core Metadata Specification” (NCMS). Default storage size is 4 GB[4].

Best for: customers who require quick delivery collaboration environment focused on common professional interest (Communities of Interests) or/and those who wish to work together with NATO External Partners.

Available on[5]:

	PUBLIC	UNCLASSIFIED	RESTRICTED	SECRET	MISSION SECRET

[1] Can be increased, based on customer requirements and subject to an additional cost of the underlying prerequisite services for the additional storage.

[2] Can be increased, based on customer requirements and subject to an additional cost of the underlying prerequisite services for the additional storage.

[3] Quick Service Instantiation applies to the case of the Internet or the NS network, were the COI is already instantiated.

[4] Can be increased, based on customer requirements and subject to an additional cost of the underlying prerequisite services for the additional storage.

[5] Depending on the Service Flavour, the Service Instantiation timelines may vary per network.

NATO Enterprise Collaboration Platform	X	X	X	X	X
Customer-specific SharePoint Collaboration Platform	X	X	X	X	X
Communities of Interests (COI) Collaboration Platform	X	X		X	

Service prerequisites[1]**:**

WPS002 Enterprise Identity Access Management Service
WPS003 Enterprise User License Service
PLT003 Web Hosting Service

Standard Service Support Levels:

Service Availability Target: 99%

Service Restoration Priority: P3.

The Standard Service support comprises the following activities:

- **Operation**: application monitoring, log management, batch jobs management, backup & restore, auditing, Service Requests fulfilment.
- **Corrective Maintenance**: diagnosis and removal of the causes and the effects of any malfunction affecting the Service.
- **Preventive Maintenance**: preventive actions needed to avoid future malfunctions
- **Adaptive Maintenance**: adjustment of the Service in order to adapt to the minor changes of the sub system components (i.e. Operating System, Database Management System, Browser, SharePoint and SharePoint add-ons). Major changes of the sub system components shall be requested via dedicated projects.

Service Cost / Price:

The unit of measure for the Service is “per URL”, and more specifically:

- In the case of the NATO Enterprise Collaboration Platform / Customer-specific SharePoint Collaboration Platform, the unit of measure is per each SharePoint “Site Collection”
- In the case of the Communities of Interests (COI) Collaboration Platform, the unit of measure is per each Community of Interest “Site”.

The price depends on the type of “Service Plan” chosen by the customer, as per the following table:

[1] Service prerequisites depend on the Network and on the specific Service Flavour.

Service Plan	**Number of registered users**	**Number of Service Requests/Year**[1]
Basic	Maximum 100	Up to 6
Advanced	Unlimited	Up to 12

The table above shows that every Service Plan enables the customers to have a maximum number of registered users and to ask for a maximum number of Service Requests per year.

The cost of the Service does not include the cost of all the underlying Service prerequisites.The total amount of the Service delivery price is charged in accordance with specifically arranged conditions of the Service delivery.

[1] Service Requests are “Category 1” changes available on ITSM. Service Requests do not include other types of changes [e.g. changes that require Change Advisory Board (CAB) approval: these changes will be requested via a Customer Request Form (CRF)].

PLT002 Combined Federated Battle Laboratory Network (CFBLNet) Service for NATO Organisations

Service ID: PLT002

Service Name: Combined Federated Battle Laboratory Network (CFBLNet) Service for NATO organisations

Portfolio Group: Platform Service

Service Description: The Combined Federated Battle Laboratories Network is a multinational, research, development, training, trials and assessment infrastructure for C4ISR, based on a multinational IP backbone with managed enclaves on top in support of the initiatives. Infrastructure reuse for multiple multinational and concurrent initiatives is a key element for the CFBLNet mission partners. CFBLNet operates as a true federation; no single nation owns the CFBLNet, where each member is responsible for provisioning and operation of its own sites and systems. CFBLNet fulfils the need for persistent joint multinational and cost effective infrastructure. The capability allows for various partnerships; CCEB, NATO, bilateral and multilateral. CFBLNet was established in 2001 and is continuously improving its services to provide the best and most cost effective federated infrastructure in support of its mission. Currently its scope consists of 38 mission partners: all 30 NATO Nations and Austria, Australia, Finland, New Zealand, Sweden, Switzerland, European Union External Action Service EEAS (EUMS) and the NATO organization. CFBLNet is open through sponsorship to additional partner nations. As a prerequisite, customers are asked for valid security accreditation and related MSAB Site and Initiative National/NATO accreditation endorsement certificates (S-, I- NAEC’s).

Value Proposition: CFBLNet provides the Multinational federated coalition network infrastructure of choice to facilitate all potential non-operational activities to support the war fighter. The single CFBLNet network infrastructure with many partners and initiatives, saves cost, increasing their quality, lower their risk and reduce setup time. CFBLNet offers an agile and fully service based non-operational network infrastructure, and operates at up to a Secret releasable accreditation level. CFBLNet provides common framework, well defined processes, security procedures and agreed technical standards.

Service Features: The Combined Federated Battle Laboratory Network (CFBLNet) Service offers the following features:

- Access points (connection to Core up to 50Mbps)
- Network Services (Routing, encryption, switching, DNS, NTP, network management, testing)
- Service Desk (3hrs/month)
- Coordination with Nations
- Coordination for NATO
- Initiative / CIIP support
- Limited email (<20 accounts)
- Chat in standing enclaves (Chat server)
- Web Services for initiatives (Microsoft Web server)

- VOIP (Cisco Voice server)
- VTC in standing enclaves (VTC MCU in RED, Pink and CUE enclaves (Acano/Cisco or other))
- SharePoint in standing enclaves (Sharepoint server)
- Data Diodes (Low-> High file transfer)
- Anti-virus / WSUS (Antivirus and Windows update servers for automatic updates (AFPL approved and regular versions)
- Simulation of CFBLNet (optional) (simulation of nation/organisational node for testing)
- Flow audit in standing enclaves
- Additional access bandwidth (optional)

Service Flavours:

1. PLT002-1: CFBLNet for NATO organizations only – BASE
2. PLT002-2: CFBLNet for NATO organizations only – Extra NKIT

A. During initiatives
B. Outside initiatives

Features	Flavour 1
	NATO Organisations
Core Access Points	
NATO Access points	●
Network Services	●
Service Desk	●
Coordination with Nations	●
Representation for sponsored nations	
Coordination for NATO	●
Initiative / CIIP support	●
Limited email	●
Chat in standing enclaves	●
Initiative Web Services	●
VOIP	●
VTC in standing enclaves	●
SharePoint in standing enclaves	●
Data Diodes	●
Anti-virus / WSUS	●

Simulation of CFBLNet (opt)	●
Flow audit in standing enclaves	●
Full local access node provisioning and operation	●
Additional access bandwidth	●

Available on:

CFBLNet NS
NS (REL)
NR (REL)
NU
NU (REL) for various NATO and Coalition communities

Service Prerequisites:

NATO Organisational subscribers: Link between NATO Organisational CFBLNet Access Node and NATO CFBLNet PoP infrastructure through NGCS/LTX. (Alternative if NCGS is not possible: leased line, satcom, alternative linkage).

The European and NATO CFBLNet NOC/PoP has link termination points at an Amsterdam (commercial DC), NATO HQ (NGCS/LTX), NCIA Mons (NGCS/LTX) and NCIA The Hague (NGCS/LTX and commercial).

Standard Service Support Levels:

Service Availability[1] Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

Nations and non-NATO organisations which would like to subscribe to “national” CFBLNet services are handled through a CRF and subsequent FFP quotation. PLT002 is not applicable to Nations and non-NATO organisations.

[1] The minimum “Monthly Uptime Percentage” for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

PLT003 Web Hosting Platform Service

Service ID: PLT003

Service Name: Web Hosting Service

Service Type: Enabling Service

Portfolio Group: *Platform Service*

Service Status: *Available*

Service Description: Web Hosting Platform Service enables fully managed and scalable hosting platforms (on-premises /off-premises) for web based solutions. The service also provides high availability, and a disaster recovery mode for customers seeking greater performance and reliability. General features of the service include: scalability, security, availability, interoperability and performance monitoring. The service is delivered as shared or dedicated flavours on one of the following supported web hosting platforms: Microsoft Internet Information Services (IIS), Apache, Oracle Web Logic and Microsoft SharePoint as a foundation in an internet/extranet environment.

Value Proposition: Web Hosting Platform Service offers multiple benefits:

- Scalability by ensuring availability of resources as the Web-based Application Service requires;
- Lower Total Cost of Ownership (TCO) of a Web-based Application Service provided through a shared and dedicated hosting model;
- Location Independence by accessibility of a Web-based Application Service from any location with Internet Connectivity, subject to security policies that would allow;
- Secure web hosting by default to prevent the any possible violations;
- No Single Point of Failure; if one service fails, the broader service can remain unaffected, ensuring service availability and reliability.

Service Features: Web Hosting Platform Service has the following features:

- Fully managed platform –dedicated or shared- , allows application owners to focus only on their application, and no need to wory about underlying environments;
- Operational support, including performance monitoring and expertise support but not limited to;
- Optional high availability and disaster recovery capabilities ensures availability and resiliency;
- Secure Web Application Services through Access Management (within the available standard options in Microsoft Internet Information Services (IIS), Apache, SharePoint, Web Logic);
- Support for standard web protocols, included but not limited to HTTPS (SSL);
- Three-tier architecture, separating presentation layer, application layer and database;
- Server side frameworks and supported middlewares, among others: Java, .NET, PHP, Ruby,
- NATO required security features and tools.
- Web/application servers: Apache and IIS;

- Provisioning of SharePoint as a foundation platform to support hosting of SharePoint based portals and applications on Intranet and Extranet.

Service Request: *Standard for all services*

Service Flavours:

- **Shared Web Hosting Platform :** A web hosting platform shared between different web sites to reduce the cost of underlying backend. Isolation and high availability is to be provided on platform level on premises and off premises (cloud). It is best for standard web sites that do not require high volumes of information, transaction, and when platform level privileges are not required.
    - **On Premises :** It is requested by amount of data size (minimum 10 GB). After the first 10 GB quota, it can be extended with 1 GB increments. High Availability is provided by default, but without disaster recovery. It is best for the web sites publishing sensitive data to NATO Enterprise.
    - **Off Premises (cloud):** It is requested by amount of data size (minimum 10 GB). After the first 10 GB quota, it can be extended with 1 GB increments with reduced rates. High Availability and Disaster Recovery are provided by default. The service rate includes underlying infra and security costs. It is best for the web sites publisihing to public on internet.

- **Dedicated Web Hosting Platform**: A dedicated web hosting platform on isolated backend is to be provided to customer to make them able to design and manage the web sites on the platform with High Availability and/or Disaster Recovery option on premises. It is best for tailored web site that requires high volumes of information, transaction, or specific administrative privileges on the platform.
    - **Stand Alone:** It is requested by amount of data size (minimum 200 GB). There is no High Availability and Disaster Recovery provided. It is best for the non business critical web sites those not requires high performance and availability
    - **With HA only:** It is requested by amount of data size (minimum 200 GB). There is High Availability implemented, but no Disaster Recovery. It is best for the web sites sensitive to performance and requires high availability.
    - **With DR only:** It is requested by amount of data size (minimum 500 GB). There is Disaster Recovery implemented, but no High Availability. It is best for the web sites that do not require high performance nor high level availability, but require quick recovery in case of loss of the service.
    - **With HA/DR** It is requested by amount of data size (minimum 500 GB). There is Disaster Recovery and High Availability implemented. It is best for the mission/business critical web sites that require high performance, high level availability, as well as quick recovery in case of loss of the service.

Available on:

NATO Unclassified

NATO Restricted

NATO Secret

Mission Secret

Public Internet Access (PIA) Gateway (Security classification up to and including NATO Unclassified)

Hybrid and Public Cloud (Security classification up to and including NATO Unclassified and NATO Restricted)

Service Prerequisites:

PLT005 Active Directory and Federation Service

PLT006 Database Platform Services

PLT010 Cloud Services Management and Integration Service

INF004 Infrastructure Virtualization Service

INF016 Infrastructure Backup Service

Standard Service Support Levels*:*

	Availability Target	**Service Restoration Period**
Shared Web Hosting		
On Premises	99.9%	8 hours (business)
Off Premises	99.9%	4 hour (wall clock)
Dedicated Web Hosting		
Without HA/DR	98.0%	27 hours (business)
With HA only	99.9%	8 hours (wall clock)
With DR only	99.0%	8 hours (business)
With HA/DR	99.9%	4 hour (wall clock)

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: Service cost is calculated based on the data size requirement. Service Unit (SU) is GB.

Please see Service Rates document for standard rates applicable to the service

PLT004 Service Oriented Architecture & Identity Management Service (SOA&IDM)

Service ID: PLT004

Service Name: Service Oriented Architecture & Identity Management Service

Portfolio Group: Platform Service

Service Status: Available

Service Description: Using the Polaris Private Cloud Infrastructure-as-a-Service (IaaS), the Service Oriented Architecture & Identity Management Platform-as-a-Service (PaaS) simplifies collaboration across the NATO Enterprise Business Applications. A platform of SOA&IDM services, based on the best of breed technology, makes this cheaper and more efficient. Our solution follows the principles of service orientation, applying them to the design of the platform services themselves, and supports the transformation of silo-based IT system into an information system that is fully aligned with the organisation, and is easily adapted to future demands.

Value Proposition: The SOA&IDM Platform will deliver reusable SOA&IDM middleware services. These services make application development simpler and more rapid, enabling easy and secure federation between NATO ecosystem applications, enhancing application innovation, maintenance and operation. As a result, it ensures that business applications across the Enterprise can efficiently and effectively respond to NATO’s operational and static needs.

Service Features: The SOA&IDM Platform will deliver:

- AGILITY: The Platform will be available on the ON and PBN networks, and will allow Functional Services (FS) to be rapidly deployed and/or reconfigured in response to Mission environment and requirements.
- INFORMATION SHARING: Information availability to the widest possible audience, thus supporting NATO's "responsibility to share". Information flows are supported between different systems, and will be agnostic of data formats.
- RISK REDUCTION: Proficient planning and control of identities and credentials for all NATO staff, while providing effective, comprehensive authentication and access management processes.
- SIMPLICITY: FS software developers in NATO will be able to focus solely on delivering capabilities that meet the needs of the users in the operational community, rather than also providing the middleware for those capabilities, including security and interoperability. This middleware is provided by the SOA&IDM Platform services.
- INTEGRATION: IT Service lifecycle automation across NATO, which will provide an integrated service delivery environment that facilitates automation, traceability, collaboration and quality assurance throughout all phases of the service delivery lifecycle.

Wave 1 aims to achieve Final System Acceptance (FSA) by Aug 2021. Work started officially on the 6 January 2020. Wave 1 will provide the following SOA&IDM Platform middleware services:

- Identities Management
- Credentials Management
- Authentication Management
- Access Management
- Messaging Service
- Mediation Service
- Configuration Management
- Event Management
- Performance and Capacity Management
- Process Automation
- Platform Environment

Service Flavours: The Service is offered as a single flavour.

Available on:

NATO Restricted

NATO Secret

Service Prerequisites:

INF004 Infrastructure Virtualization Service

INF005 Infrastructure Integration Service

INF006 NATO Enterprise Directory Service / NEDS

INF007 Infrastructure Storage Service

Standard Service Support Levels*:*

Service Availability Target: 99.9% (during Support Hours) and 99.5 (outside of Support Hours)

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 1 hour (during Support Hours) and 4 hours (outside of Support Hours).

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service flavours is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery. Please see Service Rate document for price details.

PLT005 Active Directory and Federation Service

Service Retired and became a flavour under WPS002 - Enterprise Identity Access Management Service (Former User Access Service).

PLT006 Database Platform Service

Service ID: PLT006

Service Name: Database Paltform Service

Portfolio Group: Platform Service

Service Description: Database Platform Service provides a fully managed database platform for use as an integral part of a production, testing, and/or development environment. The service provides flexible, scalable, and demand based platform, which is oriented toward central monitoring and management where underlying complexities of Database technologies (Oracle, MS SQL, MySQL and PostgreSQL) are encapsulated as a combined generic service.

Value Proposition: The Service offers the following benefits:

- Lowered Total Cost of Ownership of a database through the provision of a consolidated, standardized and volume managed database environment;
- Agility to meet NATO demands through provision of standardized, tested environments;
- Size and growth of a database monitored and provision of required capacity made to ensure continued availability and performance to meet operational needs;
- For standard use, the underlying technical complexities are isolated from the customers, technology agnostic;
- Increased security and availability through a dedicated team of experts who monitor the service

Service Features: Database Platform Service offers the user the following features:

- Database hardware capacity;
- Lifecycle management of the Database Platform;
- Database software licensing and maintenance;
- Centrally and fully managed, automated backup with point-in-time recovery;
- Software Lifecycle management for RDBMS, maintenance (including patching) and support;
- System, database and performance monitoring and tuning;
- Capacity provisioning through scalable and flexible management of available resources.

Service Flavours:

PLT006-1 Shared Database Platform : Database platform shared between different database owners to reduce the cost of underlying backend. Isolation and high availability is to be provided on platform level on premises and off premises (cloud). It is best for basic requirements that do not need high volumes of information, transaction, and when platform level privileges are not required (like sysadmin). Minimum 10 GB is provisioned.

Dedicated Database Platform: A dedicated database hosting platform on isolated backend is to be provided to customer to make them able to design and manage the data on the platform with High Availability and/or Disaster Recovery option on premises and off premises (cloud). The dedicated platform can be enabled on top of. It is best for tailored applications that requires high volumes of information, transaction, or specific administrative privileges on the platform.

PLT006-2A Stand Alone: There is no High Availability and Disaster Recovery provided. It is best for the non business critical applications those not require high performance and availability. Minimum 250 GB is provisioned

PLT006-2B with High Availability only: There is High Availability implemented, but no Disaster Recovery. It is best for the applications sensitive to performance and requires high availability. Minimum 500 GB is provisioned.

PLT006-2C With Disaster Recovery only: There is Disaster Recovery implemented, but no High Availability. It is best for the applications that do not require high performance nor high level availability, but require quick recovery in case of loss of the service. The implementation of the DR is guaranteed that not in the same data center. Minimum 750 GB is provisioned.

PLT006-2D With High Availability and Disaster Recovery: There is Disaster Recovery and High Availability implemented. It is best for the mission/business critical applicaitons that require high performance, high level availability, as well as quick recovery in case of loss of the service. Minimum 1000 GB is provisioned.

PLT006-3 Oracle Technology Product Licenses: Depending on Oracle's licensing policy, all physical processors connected to network is to be licensed. The unit of measure for this flavour is 1. The products covered are listed below. Formal request (via ITSM) is required for use.

- Oracle Database Enterprise Edition
- Oracle Real Application Clusters
- Oracle Diagnostics Pack
- Oracle Tuning Pack
- Oracle Analytics Server
- Oracle Data Integrator Enterprise Edition
- Oracle Active Data Guard
- Oracle WebLogic Server Enterprise Edition
- Oracle Database Lifecycle Management pack

Available on:

NATO Unclassified (On-Prem and Off-Prem/Cloud)

NATO Restricted

NATO Secret

Mission Secret

Service Prerequisites:

WPS002 Enterprise IDAM Service

PLT010 Cloud Services Management and Integration Service

INF004 Infrastructure Virtualization Service

INF016 Infrastructure Backup and Archive Service

APP001 Approved Commercial-off-the-shelf Products Procurement Service

Standard Service Support Levels*:*

Flavours	Availability Target	Service Restoration Period (for P0/P1 incidents)
PLT006-1 Shared Database Hosting	99.9%	8 hours (business)
PLT006-2 Dedicated Database Hosting		
PLT006-2A Stand Alone	98.0%	27 hours (business)
PLT006-2B With High Availability only	99.9%	4 hours (wall clock)
PLT006-2C With Disaster Recovery only	99.0%	8 hours (business)
PLT006-2D With High Availability and Disaster Recovery	99.9%	4 hours (wall clock)
PLT006-3 Oracle Technology Product Licenses	Not Applicable	

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Trainings (not covered by service rate):

A3045	Introduction to SQL Language
A3123	Postgre SQL Administration

Service Cost / Price:

The unit of measure for the Service flavours PLT006-1 and PLT006-2 is per GB. The unit of measure for PLT006-3 is 1.

PLT007 DCIS – Afloat Command Platform (ACP) Service

The Service has been consolidated under the INF035 DCIS – Deployable Nodes Service.

PLT008 DevSecOps Service

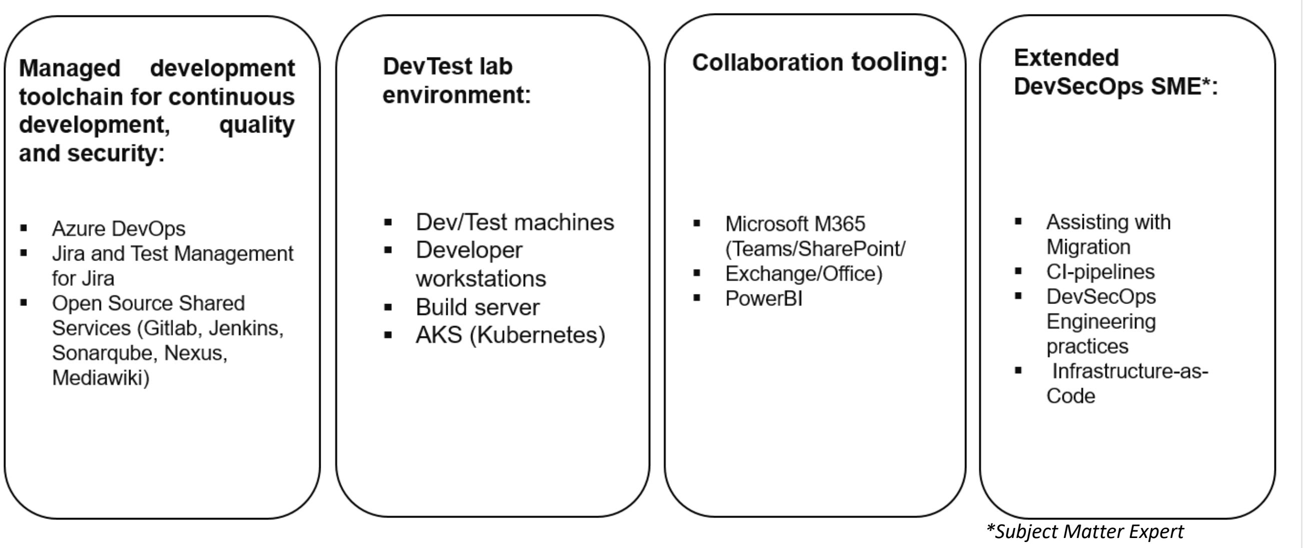
Service ID: PLT008

Service Name: DevSecOps Service

Portfolio Group: Platform Services

Service Description : PLT008 DevSecOps service is available for NCI Agency internal and external customers' needs to manage software application lifecycle.

It consists of a security accredited DevSecOps platform, which enables the NATO Software Factory (NSF) as a space for the collaboration between NCI Agency, Industry, Nations and Academia for development and test activities.



Managed development toolchain for continuous development, quality and security:

- Azure DevOps
- Jira and Test Management for Jira
- Open Source Shared Services (Gitlab, Jenkins, Sonarqube, Nexus, Mediawiki)

DevTest lab environment:

- Dev/Test machines
- Developer workstations
- Build server
- AKS (Kubernetes)

Collaboration tooling:

- Microsoft M365 (Teams/SharePoint/
- Exchange/Office)
- PowerBI

Extended DevSecOps SME*:

- Assisting with Migration
- CI-pipelines
- DevSecOps Engineering practices
- Infrastructure-as-Code

**Subject Matter Expert*

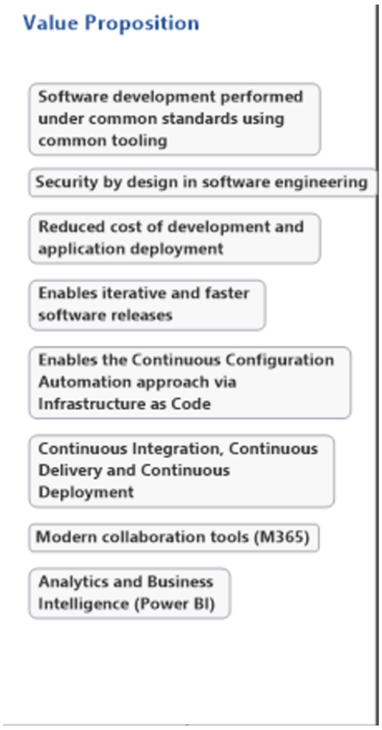
DevSecOps service key activities

PLT008 is available as Platform as a Service (PaaS) in support of the following practices:

- Requirements Management;
- Architecture & Design;
- Agile development;
- Continuous Integration (Build & Test);
- Test Automation;
- Continuous Delivery (Deploy & Release);
- Security By Design;
- Infrastructure as Code (IaC).

Value proposition:

DevSecOps service provides a secure platform, collection of best practices and expertise, tools and modern security habits that increase the ability to securely deliver applications and services at high velocity by closing the gap between development and operations. It aims to shorten the development lifecycle and provide continuous delivery with high quality.



Value Proposition

Software development performed under common standards using common tooling

Security by design in software engineering

Reduced cost of development and application deployment

Enables iterative and faster software releases

Enables the Continuous Configuration Automation approach via Infrastructure as Code

Continuous Integration, Continuous Delivery and Continuous Deployment

Modern collaboration tools (M365)

Analytics and Business Intelligence (Power BI)

Software development performed under common standards using common tools increases efficiency, continuous improvement of the product, in quality, security, reliability and coherency with operational requirements.

Security by design approach is shifting security to the left of the development cycle.

Enables fast development via techniques such as:

Infrastructure as Code enabling Continuous Configuration Automation

Continuous Integration, Continuous Delivery, Continuous (automated) Testing, Continuous Deployment

Analytics and Business Intelligence using Power BI

Modern collaboration tools via Microsoft 365

The Service brings several business benefits where:

1. The Agency and NATO stakeholders exploit the Software Factory in which development is performed under common standards using common tooling;
2. It represents mandated PFS in procurements for NSIP;
3. Through self-service cloud provisioning, suppliers working on projects or service adaptation can deploy standard environments for development, testing and regression testing;
4. These environments can be populated with test instances of all services that the component under development consumes;
5. Software development is performed with Security by Design approach taking advantage of automation to perform security policy for:
    a. Protect Credentials from theft;
    b. Scan OSS components for vulnerabilities;
    c. Red-team war games;
    d. Threat modeling;
    e. Block lateral movement;

f. Secure and Compliant Pipeline.

The benefits of the Service include:

- Enabled end-to-end traceability from the original operational requirements to the implemented solution components;
- Establish the intended collaboration (technology and practices) with Industry;
- Increased quality of FAS releases through traceability, real-time progress information, ongoing/recurring testing and through feedback loop for production incidents;
- Increased manageability through centralization and automation**;**
- Enable iterative and faster SW releases (release cadence);
- Better instruments to manage portfolio;
- Better control over IPR;
- Easier onboarding of new staff due to alignment with industry methodologies and best practices;
- Improve the efficient use of valuable resources (Staff, Infrastructure, Funds);
- Enable planned and implemented reuse of SW components;
- Reduced cost of development and application deployment (installations);
- Introduce the approach of Security by Design for software applications.

Service Features:

Access to managed and supported NSF Toolchain: The DevSecOps platform is used as development and testing environments, and it offers a series of tools (NSF Toolchain) based on both Microsoft, and Open Source Stack technology (OSS) ecosystems to ensure coherency with NATO C4ISR Application and Technology architectures. NSF Toolchain is available in Annex A.

DevSecOps SME support: Dedicated support on requestor-specific DevSecOps processes and implementation scenarios such as

- Continuous planning: Agile planning, Thread modelling, Security requirements
- Continuous integration: Test-driven development, shift-left testing, micro-services/container development, static application security scanning, secrets scanning
- Continuous delivery: infrastructure as code, release pipeline, security testing, monitoring, telemetry

Cloud Security Operations activities:

- monitoring,
- detection and response,
- event and incident response,
- continuity of operations,
- threat hunting

using cloud native tools such as:

- Microsoft Sentinel

- Microsoft Defender for Cloud
- Azure and M365 Logging and monitoring
- Various Microsoft Defenders protecting workloads (O365, endpoint, Identity, cloud apps, containers, DevOps etc)
- Azure Active Directory Identity Protection
- Endpoint detection and response (EDR) solution
- Microsoft Purview Compliance Manager

Service Flavours:

The service is available in the following flavours.

1. NSF Standard Profile: Provides access to all NSF services. This is required for most users. Typical use: Developers, Engineers, Testers.
2. NSF Stakeholder Profile: Provides access to NSF Team stakeholders without having to procure a NSF Basic User Profile. The stakeholder will be able to use VPN client to join events such as specific test events, User Acceptance Test (UAT) and Demonstrations.
3. NSF Jira Profile: Limited NSF user profile that only grants access to JIRA. Typical use: Customer representatives (JIRA based projects), JIRA project management (non-software).
4. NSF ADO Profile: Limited NSF user profile that only grants stakeholder access to Azure DevOps (allows access to wiki and work items only). Typical use: Customer representatives (ADO based projects).
5. NSF GitLab Profile: Limited NSF user profile that only grants access to GitLab. Typical use: External collaborators (e.g. partners from NATO nations).
6. NSF private cloud:
    - i. Private cloud-based platform enabling DevSecOps technology adoption in support of C4ISR information superiority
    - ii. Classified but non-operational staging environment to support NATO to test applications
    - iii. On-premises enclave for legacy workloads and specialized hardware that cannot be virtualized
7. For NSF standard profile the following services are available as additional options:
    - a. NATO Trusted Container building service
        - i. Service flavor to consume a centralized pipeline to build trusted application containers
        - ii. Security vulnerability and compliancy assessment using automated scanning tools
        - iii. Promotion to NATO Trusted Container Registry for use of containers on operational networks
        - iv. Security Validator
            1. Based on the findings, mitigations, justifications, and other relevant container characteristics, the Security Validator assigns a container image a trust level and documents any restrictions regarding its deployment
    - b. NATO Trusted Container registry consumption service

   i. Container platform to consume the NATO Trusted Container Registry on operational networks.
   ii. Requires a diode to transfer container images from low to high using 1-way diode
   iii. Centralized high-available container registry on NS

c. <u>NSF Managed Endpoint:</u> secured managed baseline for end-user devices accessing NSF resources
   i. Unified endpoint management - cloud based endpoint management, security hardening and compliance management, apps management, content management
   ii. Endpoint Protection Platform - security protection via Microsoft Defender for Endpoint, EDR (endpoint protection and response) and threat hunting integration with NSF Security Operations (SOC)

Available on:

Hybrid, Public Cloud (NU), Private Cloud (NS)

Service prerequisites:

No service prerequisites

Standard Service support levels*:*

	Availability Target	**Service Restoration Period**
During Support hours	99.9 %	2h
Outside Support hours	99.9 %	Best effort

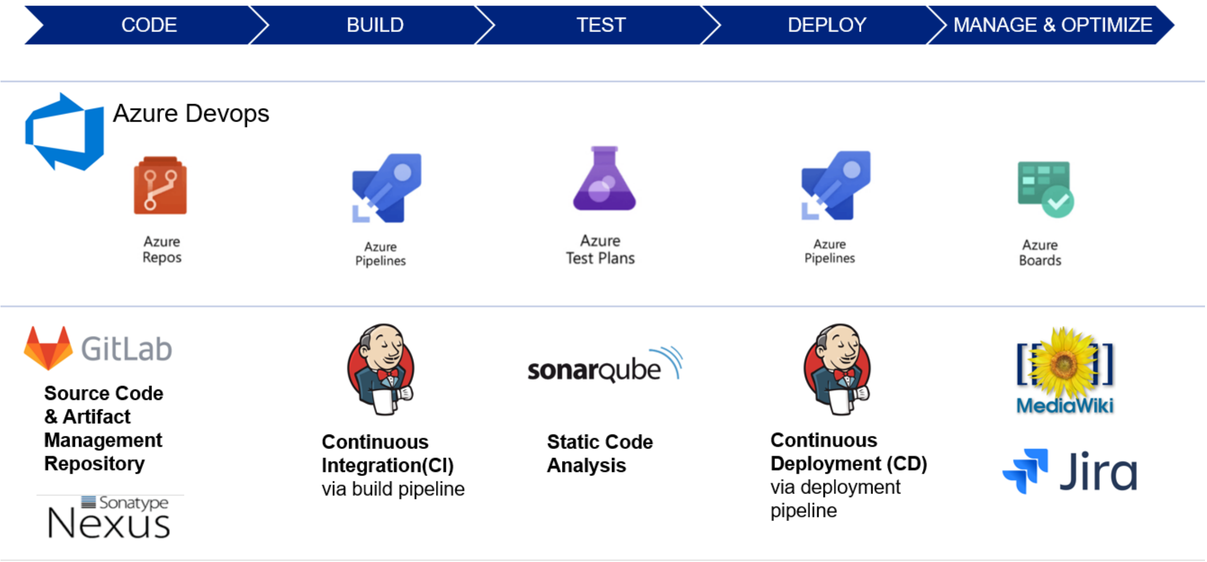
The levels in the table refers to the management and support of the NSF Toolchain. Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. The service Restoration depicts that 70% of reported incidents should be resolved in the specified timeframe.

The service is supported by incident management, service request management and on-boarding management processes details of which are available from related Service Delivery Plan and Service Support Package.

Service Cost / Price: For all PLT008 service flavours, there is a fixed license cost per user per month to cover cloud consumption costs for hosting and supporting NSF toolchain. The PLT008 costs and license costs that are part of the NSF user profiles.

Additionally, on top of either one of the flavours, PLT008 SME support can be requested. For this service, there is a fixed labour cost per hour per month to cover the manpower resources responsible to deliver the dedicated SME support.

Annex A. NSF Managed Development Toolchain



CODE BUILD TEST DEPLOY MANAGE & OPTIMIZE

Azure Devops

Azure Repos

Azure Pipelines

Azure Test Plans

Azure Pipelines

Azure Boards

GitLab

Source Code & Artifact Management Repository

Sonatype Nexus

Continuous Integration(CI) via build pipeline

sonarqube

Static Code Analysis

Continuous Deployment (CD) via deployment pipeline

MediaWiki

Jira

Service Assets – Software Descriptions		
Item	**Name**	**Description**
1	kubernetes	Kubernetes, or k8s (k, 8 characters), is an open source platform that automates Linux container operations. It eliminates many of the manual processes involved in deploying and scaling containerized applications. In other words, It is possible to cluster together groups of hosts running Linux containers, and Kubernetes helps easily and efficiently manage those clusters. These clusters can span hosts across public, private, or hybrid clouds. For this reason, Kubernetes is an ideal platform for hosting cloud-native applications that require rapid scaling, like real-time data streaming through Apache Kafka.
2	GitLab	GitLab is a Git-based platform that integrates a great number of essential tools for software development and deployment, and project management: • Hosting code in repositories with version control. • Reviewing code in Merge Requests with live-preview changes per branch with Review Apps. • Deploying personal and professional static websites with GitLab Pages. • Tracking the development lifecycle by using GitLab Cycle Analytics.

Service Assets – Software Descriptions		
Item	**Name**	**Description**
3	Jenkins	Jenkins is a self-contained, open source automation server which can be used to automate all sorts of tasks related to building, testing, and delivering or deploying software. It can be used with large variety of build systems, such as Maven, Gradle, NPM and yarn. It can be used for simple build tasks but also for complex multistage CI pipelines.
4	Jira	Jira is a family of products built to help all types of teams manage their work. Jira offers several products and deployment options that are purpose-built for Software, IT, Business, Ops teams, and more. JIRA Software allow to plan, track and release world-class software. • Bug tracking • Project management • Product management • Process management • Task management • Software development • Agile software development • Test Management
5	sonarqube	SonarQube (formerly Sonar) is an open-source platform developed by SonarSource for continuous inspection of code quality to perform automatic reviews with static analysis of code to detect bugs, code smells, and security vulnerabilities on 20+ programming languages. SonarQube offers reports on duplicated code, coding standards, unit tests, code coverage, code complexity, comments, bugs, and security vulnerabilities.
6	Nexus	Manage and store components from dev through delivery, build artifacts, binaries, containers, assemblies, and finished goods (releases and release candidates) in one central location, including intelligent staging and release functionality. Understand component security, license, and quality issues. Store and distribute Maven/Java, npm, NuGet, RubyGems, P2, OBR, APT and YUM and more. Nexus IQ and Firewall prevent vulnerable and incompliant components from entering the software supply chain, based on governance policies. When new components are downloaded, Firewall scans every new package against a set of organization-defined policies. Any component or dependency that violates one of these policies is then blocked from the repository.

Service Assets – Software Descriptions		
Item	**Name**	**Description**
7	AZURE DEVOPS	Azure DevOps Services provides development collaboration tools including high-performance pipelines, free private GIT repositories, configurable Kanban boards, and extensive automated and continuous testing capabilities. It includes: • Azure Boards • Azure Pipelines • Azure Repos • Azure Test Plans • Azure Artifacts • Extensions Marketplace
8	MediaWiki	The MediaWiki software is used by tens of thousands of websites and thousands of companies and organizations. MediaWiki helps you collect and organize knowledge and make it available to people. It's multilingual, free and open, extensible, customizable, reliable, and free of charge.

PLT009 Electronic Definitive Media Library (EDML) Service

Service ID: PLT009

Service Name: EDML Service

Portfolio Group: Platform Services

Service Description: Electronic Definitive Media Library (EDML) service is available to customers to meet the demand for media delivery. Example of media are COTS SW, NATO FAS, artefacts, graphics and documentation. The service is available from the public cloud, Microsoft Azure.

Value proposition: EDML allows exchanging data in a more flexible and secure way, with reduced “Mean Time To Resolve” (MTTR) while keeping control over access and delivery in today’s high standards of secure access.

Service Features: The Electronic Definitive Media Library provides a secure one-stop-shop for NATO software and media, accessible from anywhere in the world. It offers a number of specific benefits including user registration and controlled user access, public key encryption and access logging and auditing.

Service Flavours:

1. **NATO App Store.** Allows NATO Nations and NATO Partners, which have signed a NST Licence agreement with NATO to download NATO software tools used for testing, evaluation and operational purposes.
2. **Multi-tenant Media Delivery (SaaS[1]).** Instances of EDML enabling:
   - Data segregation between EDML instances
   - RBAC access mode with tenant administration accountability to customers whereas main root administration is ensured by the service provider
   - Upload of media via the Uploader App, which encrypts the media before the move to public cloud service provider datacentre;
   - Visibility and transparency over service cost consumption from the service provider;
   - Access the EDML Decrypter App required for the download of media.

Available on:

Public Cloud (NU)

Service Prerequisites:

None

Standard Service support levels*:*

[1] In a nutshell it means that I can have different EDMLs for different cases but that do more or less the same thing: uploading and downloading media.

Perfective, adaptive, and corrective maintenance, as well as service support and cloud resources are included.

	Availability[1] Target	**Service Restoration Period**
During Support hours	99.9 %	2h
Outside Support hours	99.9 %	Best effort

The levels in the table refers to the management and support of the EDML tenants. Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. The service Restoration depicts that 70% of reported incidents should be resolved in the specified timeframe.

The service is supported by incident management, service request management and on-boarding management processes details of which are available from related Service Delivery Plan and Service Support Package.

Service Cost / Price: The unit of measure of NATO App Store service flavour is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery. The unit of measure for the **Multi-tenant Media Delivery (SaaS)** flavour is per tenant per year with cost break as per Annex A.

[1] The minimum “Monthly Uptime Percentage” for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

PLT010 Cloud Services Management and Integration (CSMI) Service

Service ID: PLT010

Service Name: Cloud Services Management and Integration Service

Service Type: Enabling

Portfolio Group: Platform Services

Service Description: PLT010 is an enabler for public cloud based services and facilitates scalable CIS environment for NCI Agency's internal and external customers over the public internet. It operates on multiple Security Accredited Could Environments and offers robust suite of services leveraging the benefits of public cloud, such as scalability, flexibility, enhanced security and availability.

Value proposition: The Service offers the following benefits to cloud-based services or flavours:

- Scalability and Flexibility of lifecycle management of cloud resources to meet business needs;
- Security and compliance with NOS and NCSC security policies for public cloud;
- Reliability and High availability offered by cloud provider based on agreed KPIs to minimize downtime and ensures uninterrupted access to cloud resources;
- Monitoring and Performance Optimization to utilize the resource consumption to keep under control;
- Identity Access Management to secure the access with Multi Factor Authentication (MFA) through WPS002- Enterprise IDAM Service;
- Vendor Management to liaison with relevant Cloud Service Providers to assess service levels and ensure compliance with agreed-upon terms, conditions and KPIs.

Service Features:

- **Cloud Service Management and Governance**, including cloud cost management, tenant and subscription management;
- **Identity and Access Management**, including account management, conditional access, permissions and policies (through WPS002- Enterprise IDAM Service);
- **Cloud Resource Management**, including networks, subnets, VPNs, compute and storage, backups operations, IaaS, PaaS and SaaS offering of cloud provider;
- **Scalability and Flexibility**, in terms of deploying, managing and scaling resources to accommodate changing workloads and business requirements.
- **Monitoring and Performance**, including comprehensive monitoring capabilities to track the performance, availability and health of cloud resources;
- **Cloud Security & Compliance,** including hardening of the resources offered by cloud provider, as well as security monitoring and compliance;
- **Integration of the cloud-based services** into the existing Service Management and Control (SMC) processes, as well as the existing resources and services;

- **Shared Foundation** with below capabilities:
  - Capacity management (tenant wide):
    - Controlling, monitoring and optimizing resources usage to keep the cost in agreed limits,
    - Provisioning of resources, implementing and maintaining the templates (200+ products offered by Cloud provider),
    - Setting and monitoring the configured metrics like performance, resources consumption, security, availability.
  - Cost management / FinOPS (tenant wide):
    - Optimizing the cost of each subscription to stay in the agreed financial limits,
    - Migrating the resources between different groups or locations to reduce the cost or increase the saving,
    - Monitoring and controlling the cost of shared foundation service to lower the financial implications,
  - Accreditation & documentation (tenant wide & assisting subscriptions):
    - Supporting accreditation and development of document package for shared foundation, as well as subscriptions.
    - Registering any design and architecture changes on tenant level into the respective CIS Description.
    - Reviewing, updating SecOps, SOPs, SOIs and providing feedbacks for respective contracts.
  - Integration (tenant wide & assisting subscriptions):
    - Enabling platform for common and managed services as "shared foundation" at tenant level,
    - Delivering the underlying, secure and accredited shared foundation for each subscriptions,
    - Integration of new resources with shared foundation to achieve standards and to ensure governance at tenant level.
    - Enabling and configuring built-in tools for tuning, securing, logging, alerting and notification in tenant and subscriptions,
    - Automation of provisioning and configuration of resources (IaC),
    - Lifecycle management of APIs and interconnectors,
    - Providing Level-3 support for subscription, and Level-2 on tenant level,
  - Tenant management:
    - Governance of the tenant, and managing tenant level resources, including global administration,
    - Managing and controlling the global level permissions, rights of the tenants,
    - Managing lifecycle of subscriptions; assignment of customer and resources to the subscription,
    - Tagging all resources for empowering fair costing and charging the service,
  - Policies (tenant wide):
    - Ensuring the compliancy of the latest NATO regulations and best practices.
    - Implementation, monitoring and control of applied policies, like conditional access, allowed locations for resource deployments, taxonomic tag enforcement, diagnostic logs and analysis.
    - Remediation of resources non-compliant with policies.

Service Flavours: The Service is available in two flavors:

1- **MarIE (Maritime Information Exchange):** MarIE is a dedicated cloud environment for MARCOM to enable a platform for information exchange**.** The unit is "**Per User**"**:**
   - **A- Start pack (up to 50 users):** Minimum 50 users are mandatory to operate the environment.
   - **B- Additional users (> 50):** Cost of a user after first 50 with reduced price.

2- **Resource Consumption:** The cost of cloud resources varies based on consumption. It covers the costs of assigned resources (via Azure credits), the portion of the cost of the shared foundation and operation/maintenance cost. The unit measure of the service is "**Per Credit**":
   - **A- Start Pack:** Minimum 4 credits are mandatory to initiate and operate new subscriptions,
   - **B- Additional Credits:** Cost of each credit (includes 1 Azure Credit).

Available on:

Public Cloud at NATO Unclassified level.

Service Prerequisites:

WPS002 Enterprise Identity and Access Management Service

Standard Service Support Levels:

	Availability Target	**Service Restoration Period**
Support hours	Based on KPIs[1]	Based on KPIs [1]

Service Cost / Price:

1- MarIE – Maritime Information Exchange (per user)

Service ID		**Unit of Measure**
PLT010 - 1A	Start pack (up to 50 users)	1
PLT010 - 1B	Additional users (> 50) (per user/year)	Per user

2- Resource Consumption (per Credit) :

Service ID		**Unit of Measure**
PLT010 – 2A	Start Pack (min 4 Credits for creation of subscription)	Per Credit
PLT010 – 2B	Additional Credit	Per Credit

[1] Depending on the contract conditions, KPIs with Cloud Provider and/or Customer.

PLT011 Cloud Application Access (CloudApp) Service

Service ID: PLT011

Service Name: Cloud Application Access (CloudApp) Service

Portfolio Group: Platform service

Service Description: The Cloud Application Access Service provides users with the possibility to access applications in the NATO Datacentre through the use of a local web browser. The Cloud Application Access Service provides a simple web page containing icons for the applications the user can access. A centralised application provisioning allows a single point of management for the application baseline and user authorisation.

Value Proposition: The Cloud Application Access Service allows the user to securely use an application published in the NATO Datacentre from any IP connected device with a web browser. This service may be used to allow the user from the NATO Secret (NS) network to access published applications on a Mission Secret (MS) domain in the NATO datacentre (Mission Information Room, MIR) without the need for a MS workstation.

Service Features: The service features include secure web access to a web page that lists a selection of icons for every published application for each particular user. By accessing this published application, a local session (in the datacentre) starts under the credentials entered as part of the web page logon.

As the session and application data is running in the NATO datacentre, the performance for each user is identical (depending on the type of network access).

Usage, metering, and performance measures are being recorded and may be shared with the customer representative.

Service Request: Once the service is contracted by SSP/SLA, the service can be requested through an ITSM request for a single or a group of users.

As the Cloud Application Access Service needs coordination with the dependent services (IaaS/Identity) and depending services (CES/COI applications) a Service Delivery Manager (SDM) is available for close coordination with the customer. The SDM will be the point of contact for coordination planning, problem management and performance reporting which will be critical in particular as part of NRF exercises

Service Flavours:

> **MIR Cloud:** Specific flavour of Cloud Application Access Service that allows access to MS published applications from the NS network
>
> **NS/NU Cloud:** Specific flavour of Cloud Application Access Service that allows access to NS/NU published applications from the same NS/NU network. Note that the client device from which the application is accessed does not need to be managed by NCIA (f.e. BICES)

Available on: NU (PAN), MS (NRF, NMI, Op Sea Guardian), NS (AIS)

Service Prerequisites:

WPS001 Managed Device Service or a qualified device with a web browser;

WPS002 Enterprise Identity Access Management Service, the user requires a user account for the domain on which the application is published;

WPS003 Enterprise User License Service, or otherwise licensed relevant Microsoft office software;

INF004 Infrastructure Virtualization service and INF005 Infrastructure Integration Service, as the Cloud Application Access Service needs to be hosted on the NATO Data centre infrastructure;

INF007 Infrastructure Storage Service, the user requires a personal profile storage space (minimum 3 GB on default) to be able to store user profile files.

Standard Service Support Levels:

	Service Flavour	**Availability target during support hours**	**Availability target out of support hours**
Level 1	MIR Cloud	99.9%	99.5%
Level 2	NU/NS Cloud	99.5%	99.0%
	Service Flavour	**Restoration period during support hours**	**Restoration period out of support hours**
Level 1	MIR Cloud	1 hour	4 hours
Level 2	NU/NS Cloud	1 hours	4 hours

N**.B.** Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is Per Concurrent User (CCU), with a minimum number of 10 CCUs required to establish the Service on an existing CloudApp Platform (100 CCUs are required for a dedicated Platform). The price details available in the Service Rates document.

PLT012 Maritime Command and Control Platform (MARC2P) Service

This service is moved to INF035 DCIS - Deployable Nodes Service as of CCSC v9.0 as a flavour.

PLT013 NATO Integrated Secure Platform (NISP) Service

Service ID: PLT013 (old ID: APP051)

Service Name: NATO Integrated Secure Platform (NISP) Service

Portfolio Group: Platform Service

Service Description: The NATO Integrated Secure Platform (NISP) has been developed as a tool to work alongside the Oracle Solaris operating system (OS), simplifying the Solaris installation and common system administration tasks. NISP provides the means for implementing a networked platform, open to a range of applications, which ensures site installations are easier to maintain and can be supported centrally. NISP has become the standardised general purpose system configuration tool, suitable for all AirC2 applications supported by the NCI Agency.

Value proposition: NISP realizes the value at the user side by standardizing Solaris and Linux based Operating System platform installation and configuration while securing the installation in accordance with Cyber Defence mandated CIS security settings.

Service Features: The NISP Service offers the user:

- Simplified installation and maintenance of Oracle Solaris and Linux based Operating System Platform,
- Easing the tasks of the system administrator by providing a rich set of scripts for installation and administration,
- Securing these OS platforms by applying a pre-configured set-up as required for NATO networks,
- Providing security and OS patches either periodically, on demand or on request by the user,
- Standardize the Oracle Solaris and Linux based installations and configurations for easing system platform support and troubleshooting,
- Comprehensive documentation for system installation, configuration and administration,
- Supports SPARC for Oracle Solaris as well as Intel x86 based hardware for Oracle Solaris and Linux.

Service Flavours: NISP flavours that the customers can choose from are:

- Full NISP Software Baseline Maintenance and In-Service-Support (ISS) for NCS sites,
  - This service flavour is NATO common funded and includes maintenance of the NATO NISP single SW baseline which is a pre-requisite for all other service flavours which are offered through the service catalogue.
- Stand-alone server or client installations,
- Fully integrated, networked solution including NISP client and server as well as windows network integration if required.

Available on:

NATO Unclassified

NATO Restricted
NATO Secret
Mission Secret

Service Prerequisites:

INF004 - Infrastructure Virtualization Services to provide the server instance (either physical or virtual) on which a NISP server can be deployed.

Alternatively to INF004, NISP can be deployed on server and client hardware or virtual infrastructure compatible to install and run Oracle Solaris or Linux.

NISP for Solaris instances requires a license for the Oracle Solaris operating system IAW Oracle license terms and conditions.

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

Monday to Thursday: 0600 to 2200 (CET)
Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 CET).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

- Belgium +32 65 44 3177
- Netherlands +31 70 374 3177
- Italy +39 081 721 3177
- Germany +49 282 4978 3177
- USA +1 757 747 3177
- For NATO HQ +32 02 707 5858

Service Requests:

To request the INF028 - ASIM service, please complete the Customer Request Form and contact NCI Agency through the submit function included in the form following the link below. https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

NISP functional unit	Service Level Target (availability)	Performance Thresholds
Client installation	99.5%	15“ (start-up) 30” (re-start)
Server installation	99.5%	10’ (start-up) 15’ (shut-down)

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

> **N.B.** Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Available NCI Academy Training not covered by service cost:

A1000	Combined NISP ICC System Administrator (CNIC)
A1006	NISP System Administrator

Service Cost / Price: The unit of measure for all Service Flavours is 1. Service Initiation and In-Service-Support will be provided and charged in accordance with the scope and financial estimates developed and agreed through site specific Technical Agreements.

Service ID	Service Name	Service Flavour/Option	Service Unit
PLT013	NATO Integrated Secure Platform (NISP) Service	NISP software baseline maintenance and In Service Support (ISS) for NCS sites	1
PLT013	NATO Integrated Secure Platform (NISP) Service	Stand-alone Server or Client installation	1
PLT013	NATO Integrated Secure Platform (NISP) Service	Server and client installation integrated into existing networks	1

PLT014 Integration Tests Platform Service

Service ID: PLT014

Service Name: Integration Tests Platform Service

Portfolio Group: Platform Services

Service Description: The Service provides a production-like environment, tools and services based on the NATO Software Factory that enables running the mandatory integration tests for all those FAS or applications that have dependencies or interactions with other applications or core services, on the basis of automation to the maximum extent possible. In addition, this service provides the Integration testing subject matter expertise (SME) in charge of executing test plan and test cases mandatory for the contractual obligation of contractors during project implementation and during the integration activities required during the O&M of application services.

Value proposition: The Service offers the following benefits to projects by using cloud computing:

- Takes advantage of cloud service provisioning, to rapidly and cost effectively deploy readily available production-like infrastructure environments and virtual machine for applications, only available the time needed for running integration tests.
- Increased manageability through self-service, centralization, and automation;
- PLT014 is offered as PFS (Purchaser Furnished Service) for integration testing for NATO applications under procurement;
- Improve the efficient use of valuable resources (Staff, Infrastructure, Funds);
- Direct access to DevTest environments in the NATO Software Factory DevSecOps platform, taking advantage of rapid installation of relevant application releases.
- PLT014 is part of NSF services, with security accreditation granted by Security Accreditation Authorities
- Integration test toolchain support and import of test plan and test cases designed for the specific integration tests.
- Coherent with NATO Software Factory architecture and technical compliance;

Service Features:

Automated Infrastructure Provisioning, including AD infrastructure, official GPOs and security settings, VM management, patching, antivirus and related services via Continuous Integration (CI) pipeline.

Application Provisioning; deployment and configuration of applications in the infrastructure, with official releases and configuration instructions provided by application service delivery managers.

Management of toolset; Test management tooling with support from test SMEs

PLT014 FAS Catalogue: lists all core services and FAS available on PLT014 and provides for each service configuration details, version information, service end points, and points of contact.

Service Flavours: The Service is available as a single flavour.

Available on:

Hybrid and Public cloud at NATO Unclassified level that may carry administrative markings

Service Prerequisites:

PLT008 DevSecOps platform.

Standard Service Support Levels:

	Availability Target	**Service Restoration Period**
During Support hours	99.9 %	2 hours
Outside Support hours	99.9 %	Best Effort

N.B. Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table above. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The cost of the service comprises a fixed cost portion and a variable cost portion:

The fixed cost portion is mandatory for the service to exist. It is not attributable to a single project using the platform. It covers the costs required to operate and maintain the platform. It includes the manpower and expenses required for:

- Support
- Onboarding
- Patching
- Service updates (Core Services)
- Self-service portal
- Maintenance of PLT014 available services catalogue
- Service improvements

The dynamic costs are charged to each individual project based on the actual usage of the platform by that project. These costs include the Azure consumption (storage and compute) and the optionally procured Test SME support. The Azure consumption will be charged against each project's balance of Azure credits (as procured through PLT008). The Test SME support will have to be procured in advance.

PLT015 CQO Reference Platform Service

Service ID: PLT015

Service Name: CQO Reference Platform Service

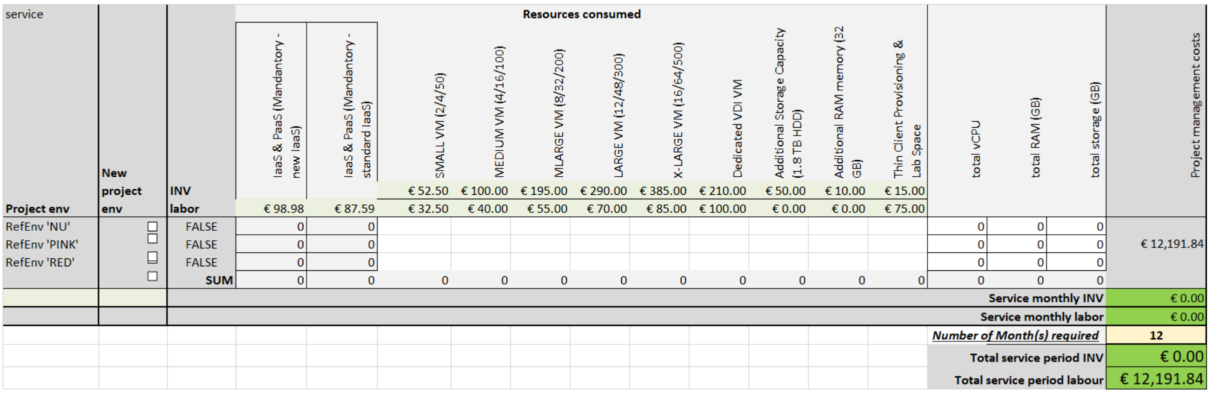
Service Type: Customer facing, Supporting and Enabling

Portfolio Group: Platform Service

Service Description: The CQO Reference Platform Service provide environments and tools in support of Interoperability testing and formal V&V for internal and external projects.

Value Proposition: CQO Reference Platform Service provides a reference infrastructure and/or Interoperability testing infrastructure to the projects, including international entities. It facilitates activities for testing, demonstration and exercises. Since the CQO Reference Platform Service is a shared infrastructure with multitude of subscribers and users and associated economies of scale, it saves cost, increases quality and lowers participants' risk by providing a standard and accurate reflection of the production environment. The CQO Reference Platform Service is complementing the CQO test services [SME002]. It provides a platform and virtual machines used in testing those products that cannot be tested in NSF. It can also be used as a stand-alone or supporting service in other projects and programmes. CQO Platform Reference Service offers an agile and fully service based non-operational infrastructure, and operates at up to a Secret releasable accreditation level. CQO Platform Reference Service provides common framework, well-defined processes, security procedures and agreed technical standards.

Service Features:



service			Resources consumed														
			IaaS & PaaS (Mandantory - new IaaS)	IaaS & PaaS (Mandantory - standard IaaS)	SMALL VM (2/4/50)	MEDIUM VM (4/16/100)	MLARGE VM (8/32/200)	LARGE VM (12/48/300)	X-LARGE VM (16/64/500)	Dedicated VDI VM	Additional Storage Capacity (1.8 TB HDD)	Additional RAM memory (32 GB)	Thin Client Provisioning & Lab Space	total vCPU	total RAM (GB)	total storage (GB)	Project management costs
	New project	INV			€ 52.50	€ 100.00	€ 195.00	€ 290.00	€ 385.00	€ 210.00	€ 50.00	€ 10.00	€ 15.00				
Project env	env	labor	€ 98.98	€ 87.59	€ 32.50	€ 40.00	€ 55.00	€ 70.00	€ 85.00	€ 100.00	€ 0.00	€ 0.00	€ 75.00				
RefEnv 'NU'	□	FALSE	0	0										0	0	0	€ 12,191.84
RefEnv 'PINK'	□	FALSE	0	0										0	0	0	
RefEnv 'RED'	□	FALSE	0	0										0	0	0	
	□	SUM	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
																Service monthly INV	€ 0.00
																Service monthly labor	€ 0.00
																Number of Month(s) required	12
																Total service period INV	€ 0.00
																Total service period labour	€ 12,191.84

Service Flavours: The service will be adapted to the customers resource and hosting requirements and classification/releasability level.

The Test Tool Sub-Service will be adapted to the size of the user community.

Available on: NS Ref., NU-IVV-Ref, and applicable CFBLNet enclaves (e.g. CUE, RED, PINK). NU Environment accessible through Reach capability.

Service Prerequisites: NCIA subscribers: Technical Work Area (TWA) / Facility space with (diskless) workstation and connected to the CQO service infrastructure as required.

Standard Service Support Levels:

Service Availability Target: During Initiates, depend on the underpinning environments and underpinning contracts though 99 % is a minimum target.

Service Restoration: Service response time during business hours 9 Business hours. Where the service is deemed unavailable, the service restoration period for a critical incident is 18 Business hours. (Better can be negotiated)

N.B*.* *S*ervice is a non-operational service as such will have a lower resilience and availability.

Service Cost / Price: The overall services cost is calculated on a case-by-case basis for the subscriber of the shared service. The calculation principle is summarised in the table under service features section.

PLT018 Data Science Platform as a Service

Service ID: PLT018

Service Name: Data Science Platform as a Service

Portfolio Group: Platform Services

Service Description: This layer provides a Data Science Platform as a Service (DS-PaaS) combines Data Science infrastructure (DS-IaaS) with a library of software tools, exposed to scientists and analysts as services, allowing for all phases of data exploration and exploitation. The tools include common open-source tool sets, NATO-owned tool sets, commercial tool sets and hosted models (i.e. Large Language Models). It also allows for eco-system partners to bring in custom tools for hosting in the environment where these bring specific capabilities or benefits. Included in the library are data preparation tools, normalisation tools, machine learning tools, big data tools, artificial intelligence tools, data ingestion and processing tools, etc., a selection – depending on the profile – being preinstalled for a jump start.

Value proposition: The Service offers the following benefits:

- Access to a range of tools to allow exploration and exploitation of data sets.
- Development of machine learning, based on available datasets.
- Use of a range of open source and NATO-specific libraries.
- Expert support from data scientists.

Service Features: Data Science Platform as a Service offers the user the following features:

- Model development, training and implementation;
- Data pipeline development and implementation;
- Workflow development and implementation;
- Data visualisation and dashboard development.

Service Flavours:

- Data Science profile
- Advanced Analytics profile
- Machine Learning profile
- BigData (extension) profile

Available on:

NATO SECRET, classification up to including NS

Service Prerequisites:

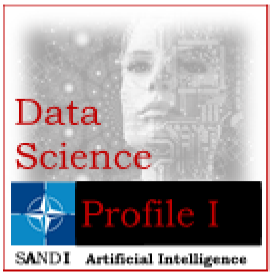
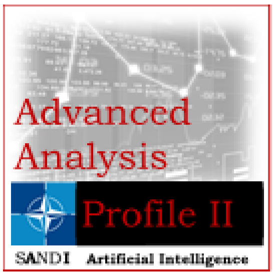
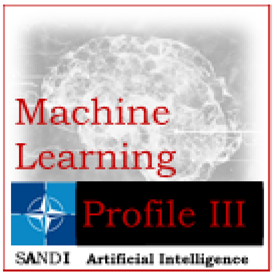
WPS001 for NS services.

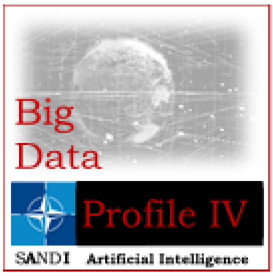
Service Availability Target : 98%

Service Restoration Priority : P3

N.B. This service is not intended to support operational or business users directly.

Service Cost / Price: The unit of measure for the *S*ervice flavours is per unit. Initial fee for subscribing to the service applies. There is an additional cost per named user of the profile(s); additional costs apply only one time if subscribing to multiple Data Science services hosted in SANDI. There is a mandatory monthly fees per named user (Advanced PaaS user profile). User profile required for those working on virtual machines (IaaS or PaaS) on NATO SECRET Data Science Infrastructure.

Profile	Description	Unit
	Data Science Profile Package of suitable software and machine configurations for Data Science teams. Combination of CPU and GPU heavy machines and powerful pre-installed software to handle data pre-processing, advanced analytics, machine learning and visualization.	Includes equivalent of 2 units of DS-IaaS: 1x Medium (⊞) 2x Medium w/ GPU (🎩) Preinstalled software: MS Office, Power BI Desktop, KNIME Analytics Platform, Anaconda (Python 3|Jupyter Lab), VSCode, SQL Management Studio, Docker
 Advanced Analysis Profile II SANDI Artificial Intelligence	Advanced Analytics Profile Package of software and machine configurations with a focus on (visual) analytics, supporting processing and analysing larger data sets quickly. Still provides more than enough GPU power to run inference and fit models to data sets.	Includes equivalent of 1 units of DS-IaaS: 1x Medium+ (⊞) 1x Small w/ GPU+ (🎩) Preinstalled software: MS Office, Power BI Desktop, KNIME Analytics Platform, Anaconda (Python 3|Jupyter Lab), R-Studio, SQL Management Studio
 Machine Learning Profile III SANDI Artificial Intelligence	Machine Learning Profile Package of software and machine configurations with a focus on machine learning, supporting model engineering, data preparation and training. Still provides more than enough resources to perform visual data analysis on top.	Includes equivalent of 1 units of DS-IaaS: 1x Small (⊞) 1x Medium w/ GPU (🎩) Preinstalled software: MS Office, Power BI Desktop, KNIME Analytics Platform, Anaconda (Python 3|Jupyter

		Lab), SQL Management Studio, Kubernetes
 Big Data Profile IV SANDI Artificial Intelligence	Big Data Profile Kubernetes node ready for distributed data processing tasks, extending a Data Science, Advanced Analytics or Machine Learning profile.	Includes equivalent of 1 units of DS-IaaS: equivalent of: 4x Small w/ GPU () Preinstalled software options: KNIME Executor, Anaconda (Python 3), Kubernetes, Spark

This page is left blank intentionally

Subject Matter Expertise (SME) Services

This page is left blank intentionally

SME001 Chief Quality Office Subject Matter Expertise Service

Service ID: SME001

Service Name: Chief Quality Office Subject Matter Expertise Service

Portfolio Group: Subject Matter Expertise Services

Service Description: The main objective of this service is to develop and maintain common framework for all Test, Verification and Validation (TVV), as well as, Quality Assurance (A) and Operational Acceptance activities, covering the full lifecycle in support of the Customer. The goal of SME001 is to ensure the quality of services, systems and products prior to deployment in the live environment.

The service supports the projects and Customer from inception to Operational Acceptance by:

- Quality and test planning.
- Assuring project documentation (PP, SoW, Plans Reports);
- Verifying project deliverables and requirements compliance;
- Providing independent risk assessment at each stage of the Project Life Cycle;
- Conducting process conformance reviews;
- Providing assurance of the Test Events led by the Contractors, and
- Provide TVVA reports and recommendations.

Operational acceptance is unique because it begins during project but continues through transition to service. This part of SME001 supports the project for Operational Acceptance requirements and activities by interfacing with the Senior Requirements Owner and ACO SHAPE J6. This is performed on behalf of the NCI Agency and the project, for OA process execution, conducted from project proposal to JFAI preparation.

Value Proposition: The purpose of SME001 is to ensure the quality of products, services and systems, as well as the projects in context of which it is developed and implemented. It is focused on improving customer satisfaction regarding NCI Agency deliverable.

Independent V&V provides an impartial assessment of whether or not the output of a given activity satisfies the customer requirements (fit-for-purpose) of that activity and that the non-functional requirements perform in the intended production environment (fit-for-use). V&V and Assurance are undertaken at every stage of the lifecycle. It enables early defect and deficiencyidentification and correction, in order to minimise their impact on cost and schedule.

Service Features: SME001 offers the user:

1. Support Type B Cost Estimate (TBCE) / Project Proposal (PP), as well as IFB Package Development;
2. Support to requirements development and review to ensure testability;
3. Independent witness ofFactory/System/User Acceptance phase provision;
4. Independent V&V and Assurance of functional and non-functional requirements
5. Quality assurance support along the project lifecycle.

6. Assistance to BA/FA regarding quality control activities consistent with the Agency Quality Management System (QMS).
7. Operational Acceptance process execution support by coordinating with and and acting on behalf of ACO SHAPE J6 to provide the Verifiable Objective Evidence (VOE) for project’s Operational Acceptance criteria fulfilment.
8. Optional support to the PM or programme with SME, technical resources or policy/process/procedural assistance:
    - Provide assistance to project/engineering testing.
    - Provide assistance with test management tools.
    - Provide support to integration testing.
    - De-risking test.

Service Prerequisites:

None

Service Flavours: The Service is available as a single flavour.

Available on:

NATO UNCLASSIFIED
NATO RESTRICTED
NATO SECRET
MISSION SECRET

Standard Service Support Levels: N/A

Available NCI Academy Training not covered by service cost:

A3076	ISTQB Certified Tester: Foundation Certification Exam Prep
A3094	ISTQB Advanced Test Manager Certificate
S7-137	NATO Quality Assurance Course
T004279	Certified Quality Engineer

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SME002 Independent Verification and Validation for A2SL Service

Service ID: SME002

Service Name: Independent Verification and Validation for A2SL Service

Portfolio Group: Subject Matter Expertise Services

Service Description: The Independent Verification and Validation Service for A2SL provides a consistent and independent way of verifying and validating products and systems.

The trigger for this service is a Change Request (CRQ) submitted to the Change manager in the Service Management and Control (SMC) Functional Area.

CRQs in scope for this service are only those concerning currently fielded software and systems already available on the NCI Agency Approved Software List (A2SL). The addition of new products and systems should be funded through:

- Projects for those delivered as part of a capability for which a project exists
- CRF for external customers
- Agency funding for internal Agency customers

Value proposition: The activities, which are part of this service are performed in order to provide objective evidence that the software or system under test is of satisfactory quality and meets customer, technical and security requirements.

The tests will allow to identify issues and defects and enable them to be corrected in order to reduce the risk of end-users finding failures when the system will be deployed in the live NU and NS NATO environments.

Service Features:

- **A2SL Service Management**: This package is mandatory and contains the effort required to manage the IVV service, attend the relevant Change Management Boards (CAB), review all CRQs and evaluate the type of IVV Service required for the given CRQ.

- **CRQ Reference Environment Operation and Maintenance**: This package is mandatory and contains the effort required to maintain the environments to support all IVV activities. This includes regular maintenance and upgrades, including license management, patching, security configuration and continuous alignment of the IVV to the operational environments.

- **Operating Systems Testing:** This package will consist off the effort required to test new operating systems and new versions of approved operating systems in order to integrate it in the NATO Environment. The main effort is focused in compatibility with the existing NATO environment, and the correct function of the operating system under NATO security settings and security mechanisms. This does not include the effort needed for cyber security testing as this is in the remit of the NCSC business area.

- **Patch Testing:** This package will consist off the monthly effort required to cover the testing of patches, which submitted monthly by vendors, in order to integrate it in the NATO Environment. Testing will include:
    - Patches applied to current baseline in A2SL of Windows client and server operating systems and their compatibility with the existing NATO environment under NATO security settings and established security mechanisms.
    - Patches applied to current baseline in A2SL of Linux client and server operating systems and their compatibility with the existing NATO environment under NATO security settings and established security mechanisms.

  Cyber security testing is not in scope of this service

Commercial of the Shelf (COTS) Application Testing - Small: This package will consist off the effort required to test a new version of an already approved COTS application in order to integrate it in the NATO Environment. Small COTS applications are simple applications without any interoperability with other COTS or NOTS systems. Testing will include:

- Installation and configuration of the COTS
- Compatibility testing with the existing NATO environment, and the correct functioning under NATO security settings and security mechanisms.
- Compatibility testing with basic set of applications that will be utilized in the operating system
- Perform Test Readiness Review
- Drafting Test Report
- Perform Software Test Review
- Drafting System Administration Notes
- Any other activities to support the testing

Cyber security testing is not in scope of this service

- **Commercial of the Shelf (COTS) Application Testing - Large:** This package will consist off the effort required to test a new version of an already approved COTS application in order to integrate it in the NATO Environment. Large COTS applications are complex as they contain interoperability with COTS or NOTS systems or are complex in scope due to the functionality they provide. Testing will include:
    - Installation and configuration of the COTS
    - Compatibility testing with the existing NATO environment, and the correct function of the operating system under NATO security settings and security mechanisms.
    - Compatibility testing with basic set of applications that will be utilized in the operating system
    - Perform Test Readiness Review
    - Drafting Test Report

  - Perform Software Test Review
  - Drafting System Administration Notes
  - Any other activities to support the testing

Cyber security testing is not in scope of this service

SME003 Interoperability Verification and Validation Service

Service ID: SME003

Service Name: Interoperability Verification and Validation Service

Portfolio Group: Subject Matter Expertise Service

Service Description: Interoperability Verification and Validation Service (referred to as IO V&V Service) provides a consistent way of planning, executing, reporting and evaluating interoperability events. The service has four pillars:

(1) Manpower: providing interoperability skills, experience and expertise to identify how to best verify and validate interoperability from a technical perspective. Several profiles are available, ranging from Interoperability Director, Test Directors, Test Management and IO Toolset support.

(2) Process: providing a consistent and repeatable way to perform CIS planning for a mission or event and to plan, execute and report V&V.

(3) Content: providing a common and baselined repository of V&V and CIS planning information that is reusable per mission and event

(4) Technology: providing the IO Toolset that will support the above three pillars.

As of today, the Interoperability Verification and Validation Service, with the four pillars, is managed by IV&V SL personnel and it encompasses the significant repository of knowledge gained through many years of interoperability testing which has been successfully proven in interoperability testing events.

Value Proposition: The IO V&V Service would provide benefits to every interoperability event, exercise, FMN Confirmation event and mission by assuring that there is a single process and supporting tooling that allows consistent and repeteable IO V&V assessments. Furthermore, it would allow for a comparison of individual assessments against each other across multiple events (exercises/FMN Confirmation/ missions) .

The IO V&V Service re-uses content that is being developed by Subject Matter Experts within NCI Agency, as well as the Information Exchange Requirements developed by the operational community and the repository by the FMN CIAV Working Group.

The IO V&V service and more specific the IO Toolset fills a gap that currently exists within NATO concerning CIS planning tool support and it supports a Service Management Authority (SMA) in the design of the services in the network and to automatically create the corresponding JMEI's vol IV.

In addition the IO Toolset is able to capture all the asset data and create a baseline per exercise or mission which can be the basis to enable change management.

Finally the IO V&V service would support the full lifecycle of an exercise or mission by providing CIS planning support. It would further support to the Design Authority (SMA) of the network, and execute interoperability verification and validation during the mission instantiation while supporting the change management under the lead of the Operating Authority (SMC)

Service Features:

Foundation Package

Every customer requires the foundation package that will give them access to the IO Toolset, the process, and the most up to date content ready to be used in the IO Toolset. This package will also include manpower for active toolset support during the execution of an event under the guidance of either the customer or the team contracted as part of the Execution and Reporting Service.

On-demand Services

The following on-demand services are foreseen, which will require as a precondition the foundation package.

Planning Service : Manpower support for performing CIS and V&V planning. This will provide the customer support in planning the services for the mission which will lead to a service design including the necessary set of Joining Membership and Exiting Instruction (vol. IV) which are vital to manage the services in the network. It will also provide the customer with a detailed test plan to assure the service design and implementation can be verified and validated. Besides the test plan, all the test executions are planned in the IO Toolset, ready to be executed.

Execution and Reporting Service: Manpower support for directing the execution by also implementing a complete testing organization which will lead the overall execution of all the tests. This will be done according to the needs of the customer. The customer will be assigned a complete event team consisting of an Interoperability Director and one or more Test Directors. After the event, all the results will be fully analysed and and C3 Interoperability assessment will be provided to the customer, both paper based and digitally within the Toolset. The reporting service also provides the option for an evaluation team to create, update manage and assess the exercise/ mission based on exercise objectives/ training objectives and evaluation criteria throughout the event.

Continued support throughout the lifecycle of the Mission Network: This service will require, in addition to the foundation package, the planning service and the execution and reporting Service. This manpower will be able to continue to support changes to the network after the specific initial V&V has been completed.

Training Service: This service provides options to get basic user training for participants on how to conduct testing. A part from basic training there is the option for advanced training which can be scheduled and tailored based on the individual needs of the customer. Topics are support for creating test plans, running events, creation of JMEI's and evaluation training.

Service Request: Service should be requested through a CRF, or by a SLA

Service Flavours: The Interoperability service is tailored to meet individual needs of a customer. Customization and a combination of the different packages will be possible. Foundation package is mandatory with every request.

Available on: N/A

Service Prerequisites: N/A

Standard Service Support Levels*:* N/A

Service Cost / Price: Cost for each defined effort is individually calculated, in accordance with agreed scope and conditions of the service delivery, as well as valid NCI Agency Customer Rates.

SME004 Provision of Subject Matter Expertise for the Federated Mission Networking (FMN) Framework

Service ID: SME004

Service Name: Provision of Subject Matter Expertise for the Federated Mission Networking (FMN) Framework

Portfolio Group: Subject Matter Expertise Services

Service Description: This service provides:

- Subject Matter Experts (SME) to the ACO funded portion of the management and working group structures that support the direction and development of the FMN Framework. [SLIN13.1]
- Support to derisking of the implementation of federated capabilities through collective and federated CIAV testing with Nations Affiliated with the FMN Framework.

Value Proposition: With NAC approval of NFIP Vol 1 on 29 January 2015, NATO committed itself to be the key contributor to and facilitator of the FMN Framework. ACO, ACT and IMS provide annual funding to NCI Agency to provide SME to support their respective responsibilities within the FMN Framework. This service is to maintain ACO's portion of the NATO funded support to the FMN framework and its organizational structure, as directed by the MC and subsequently approved by the NAC. The maintenance of ACT's portion of the NATO funded support to the FMN framework and its organizational structure is funded via the ACT POW. The support provided to help ACO represent the NATO Command Structure as an Affiliate to the FMN Framework (NCSaaA) is provided via SME009.

Service Features: The Service provides the following areas of expertise and facilities:

- **Support the FMN Secretariat**.
  - Provision of Change Implementation Coordinator (CIC) within the FMN Secretariat;
  - Provision of unclassified DNBL FMN portal infrastructure to the FMN Secretariat for the governance and management bodies of the FMN initiative and the Coalition Interoperability, Assurance and Validation Working Group (CIAV WG);
  - Provision of FMN Architect within the FMN Secretariat.

- **Support the FMN Operational Coordination Working Group**.
  - Provision of Operational Analyst/Business Process Analyst to OCWG to assist in the definition of operational processes from Allied doctrine to identify information exchange requirements and functional and non-functional requirements;
  - Provision of support for OCWG repository to maintain alignment of data model, modelling conventions and artefacts across FMN Framework products;

  - Provision of Operational Analysis expertise to OCWG to support the preparation of products with the chair FMN OCWG and to provide linkage to the NATO Defence Planning Process (NDPP).
- **Support the FMN Multinational CIS Security Management Authority**.
  - Provision of Cyber Security expertise to the MCSMA WG meetings to assist in the preparation of federated security documentation (e.g. the template for the Community Security Requirements Statements (CSRS)) as it relates to each FMN Spiral Specification;
  - Provision of Cyber Security expertise to the MCSMA workshops to include fulfilment of tasks received after the escalation of risks to the Military Committee (MC) regarding the misalignment between NATO Security Policies and FMN Goals;
  - Provision of technical coordinator to the MCSMA to ensure consistent integration of CIS Security products across FMN Framework products of a Spiral;
  - Provision of support for MCSMA WG repository to maintain alignment of data model, modelling conventions and artefacts across FMN Framework products;
  - Provision of updated FMN Security Risk Assessment (SRA) using methodologies and tools provided by SHAPE (SRA).

- **Support the FMN Coalition Interoperability, Assurance and Validation (CIAV) Working Group**.
  - Coordinate between CICWG and CIAVWG on RFC tasked to FMN CIAVWG, including planning within CIAV WG
  - Provision of support to Framework with tools for event planning, executing and reporting, repository development and maintenance, as well as tracking RFCs;
  - Provision of IV&V SME support to Framework with development of the technical AV&V content (Spiral Instructions) including Repository management;
  - AV&V Repository Management and development of AV&V content to support CIAV objectives;
  - Provide white cell services on the CFBLnet Pink enclave for support of CIAV events.

- **Support the FMN Change and Implementation Coordination Working Group**.
  - Provision of Service Engineering SME and Service Management Expertise to provide advice on templates for the Joining, Membership and Exit Instructions;
  - Provide Naming and Registration Authority (NRA) for the FMN Framework to maintain ASN and IP Ranges assigned to the Affiliates and to respond to enquiries and help resolve conflicts;
  - Provision of System Engineer/Change Manager for FMN Baseline;
  - Provision of support for CICWG repository to maintain alignment of data model, modelling conventions and artefacts across FMN Framework products.
- **Travel:** Due to the meeting schedule of the FMN initiative and its working groups, there is considerable Travel associated with this service.

Service Request: The service can only be requested as follows:

- ACO funded: via the CSLA (SLIN13.1 and Activity 525);

Service Flavours: The service comes as a complete package and is originally based on the scope of ACO funded tasks and funding levels described in 6300/TSC-FCX-0010/TT-140441/Ser:NU1023 dated 7 NOV 14. Over the intervening years this has evolved to keep pace with demand and those tasks pertaining to NATO Command plt0plt008Structure as an Affiliate to FMN Framework (NCSaaA) have been split out from SME004 into SME009.

Available on: The SME provide the following types of service to ACO through the following networks:

- Support to FMN Management and working group structures that support the direction and development of the FMN Framework: Unclassified (DNBL FMN Secretariat Portal)/NR (Advice)/NS (Advice)
- Support to derisking of the implementation of federated capabilities through collective and federated CIAV testing with other Affiliate Nations: Unclassified (DNBL CIAV Portal)/NR (Advice)/NS (Advice)/CV2E (federated CIAV laboratory).

Service prerequisites: N/A

Standard Service Support Levels*:* N/A

Available/Related NCI Academy Training not covered by service cost:

A0104	NATO CIS Planning

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery. The service charge should take into account the extensive TDY commitment.

SME005.1 Acquisition Life Cycle Cost Estimating (LCCE) Service

Service ID: SME005.1

Service Name: Acquisition Life Cycle Cost Estimating (LCCE) Service

Portfolio Group: Subject Matter Expertise Services

Service Description: The Acquisition Life Cycle Cost Estimating Service encompasses all activities related to LCCE, such as estimation, evaluation, options development, analysis of alternatives, predictive modelling, risk analysis, forecasting and simulation. It applies to the entire range of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) and Cyber Defence projects and programmes, and includes developments in the fields of Information Technology and/or Communications and Information Systems (IT/CIS), System Engineering (SE) and hardware (HW) systems.

The Acquisition LCCE Service and resulting products are in line with the NATO Costing Practices and follow the best practice of latest governmental guidelines, formats and standards from across NATO nations.

Related Acquisition Cost Analysis and Estimation services are: Software Intensive Projects Cost Estimating (SME005.2), Cost Analysis (SME005.3) and Miscellaneous Cost Estimating & Analysis (SME005.4).

Value proposition: The Acquisition LCCE Service provides independent and unbiased cost estimating activities for the provision of capability and/or system development projects and programmes. It enables transparency and allows the Customers to secure impartial cost estimation, verification and validation. By doing so, it empowers the Customers to better determine and prioritize their needs, make informed investment decisions and to efficiently plan and manage the resources. As a result, the Customers are better prepared to effectively execute acquisition projects, support them and remain in control throughout their lifecycle.

Service Features:

Preparation of cost estimates;

Evaluation of existing cost estimates;

Development of costing options;

Analysis of Alternatives (AoA);

Analysis of multi-criteria options with TOPSIS;

Development of budgets;

Risk analysis;

Predictive modelling, forecasting, simulation and optimization;

Validation of the Project Service Costs (PSC);

Sensitivity, risk and uncertainty analysis performed on estimates to ensure the appropriate amount of funding.

Service Flavours:

Life Cycle Cost Estimating (LCCE) – Provides a cost and schedule estimate (usually parametric) for budgets of NATO and/or national projects and programmes across their lifecycle. Delivers an independent verification and validation of existing estimates; Status: Available now;

IT/CIS systems supporting Workplace Services, Application Services, Logistics Support Services, Infrastructure Services, Platform Services, Security Services, Training Services and other Services offered by the NCIA Service Lines;

Hardware based systems and integrated product assemblies costing;

Systems engineering (SE) costing based on system architecture and requirements.

Products and the enabling tools:

Product/Service	Tool/Method
LCCE including ongoing support costing, Operation and Maintenance (O&M) for all Information Technology/Communications and Information Systems	SEER IT
LCCE including ongoing support costing, Operation and Maintenance (O&M) for HW based systems and product assemblies	SEER HW
Systems Engineering costing based on system architecture and requirements	SEER SE
Predictive modelling, forecasting, simulation, and optimization, Monte-Carlo	Crystal Ball
Parametric modelling, simulation	R for Windows
Option analysis and risk prioritisation	TOPSIS
Cost estimates for NATO funded projects (TBCE, Project Proposals), RAM-Cost estimates	MS Excel

Available on: No network security dependency and/or restrictions.

Service Prerequisites: Customers will be required to provide the following information to the cost estimating service including but not limited to:

Scope definition based on a clear set of requirements;

Schedule of Supplies and Services (3S) (if available) listing the contract Deliverables, the quantities required, the location and the date of delivery;

Statement of Work (SOW) (if available) with the specification of work to be done;

Work Package (WP) (if available) definition;

Acquisition method.

The Price Proposal will detail the exact timelines and prerequisites. Where no data will be available, a set of assumptions will be developed and incorporated in the estimates.

Standard Service Support Levels: N/A

Service Cost / Price: Acquisition Life Cycle Cost Estimating Service will be costed based on level of effort (LOE). The Service delivery cost will be charged in accordance with specifically arranged conditions for the delivery. The LOE is estimated based on the requirements and subject to Customer agreement.

SME005.2 Acquisition Software Intensive Project (SIP) Cost Estimating Service

Service ID: SME005.2

Service Name: Acquisition Software Intensive Project (SIP) Cost Estimating Service

Portfolio Group: Subject Matter Expertise Services

Service Description: The Acquisition Software Intensive Project (SIP) Cost Estimating Service encompasses all activities in relation to Life Cycle Cost Estimating of SIPs including software sizing.

All products and activities performed within this Acquisition SIP Cost Estimating Service are in line with the NATO Costing Practices. They follow the best practice of latest governmental guidelines, formats and standards.

Related Acquisition Cost Analysis and Estimation services are: Life Cycle Cost Estimating Service (SME005.1), Cost Analysis Service (SME005.3) and Miscellaneous Cost Estimating & Analysis Service (SME005.4).

Value proposition: The Acquisition SIP Cost Estimating Service supports the provision of Software Intensive Projects. Its activities can be subdivided into:

software requirements analysis in terms of their usefulness for the purpose of software sizing;

software sizing, either detailed based on the full Function Point Analysis (FPA) or Early and Quick FP (E&QFP) based on indicative FP count when detailed requirements are not yet available or based on Source Lines of Code (SLOC) for existing software;

software cost and schedule estimating both for investment and for maintenance.

The Service provides transparency and enables the Customers to secure independent requirements analysis, size estimation and cost estimation. By doing so, it empowers the Customers to better determine and prioritize their needs, to make informed investment decisions and to efficiently plan and manage their resources. As a result, the Customers are better prepared to effectively execute acquisition of the Software Intensive Projects, support them and stay in control of those projects throughout their lifecycle.

Service Features: Software requirements analysis in terms of the usefulness for the software sizing;

Software size estimating as input to life cycle cost estimates, this size estimating can be performed as a full FP count, as an indicative FP count or based on SLOCs;

Software cost and schedule estimating for delivery and maintenance of software, performed both as detailed estimating and as an indicative estimating in an early stage of a project.

Service Flavours:

Software requirements analysis with relation to pricing; Status: Available now;

Software sizing, detailed and indicative Function Point Analysis (FPA), Source Lines of Code; Status: Available now;

Life Cycle Cost Estimate (LCCE) - cost and schedule estimate to support financial planning of Software Intensive Projects throughout their lifecycle; Status: Available now.

Products and the enabling tools:

Product/Service	Tool/Method
SW Sizing through Function Point Analysis	FPA
SW Sizing through Source Lines of Code	COCOMO
Project and maintenance costs and schedule for SW development	SEER SEM
Cost estimates for NATO funded projects (TBCE, Project Proposals), modelling	MS Excel

Available on: No network security dependency and/or restrictions;

Service Prerequisites: Customers will be required to provide the following information to the cost estimating service including but not limited to:

Scope definition based on a clear set of requirements;

Services (3S) (if available) listing the contract Deliverables, the location and the date of delivery;

Statement of Work (SOW) (if available) with the specification of work to be done;

Work Package (WP) (if available) definition;

Acquisition method.

The Price Proposal will detail the exact timelines and prerequisites. Where no data will be available, a set of assumptions will be developed and incorporated in the estimates.

Standard Service Support Levels: N/A

Service Cost / Price: Acquisition SIP Cost Estimating Service will be costed based on level of effort (LOE). The Service delivery cost will be charged in accordance with specifically arranged conditions for the delivery. The LOE is estimated based on the requirements and subject to Customer agreement.

SME005.3 Acquisition Cost Analysis (CA) Service

Service ID: SME005.3

Service Name: Acquisition Cost Analysis (CA) Service

Portfolio Group: Subject Matter Expertise Services

Service Description: The Acquisition Cost Analysis Service offers price analysis in support of capability and/or system development. It encompasses all activities related to Competitive Bid Price Evaluation and Non-competitive Bid Price Evaluation – optionally also including Price Negotiation Support.

All products and activities performed within this Acquisition CA Service are in line with the NATO Costing Practices. They follow the best practice of latest governmental guidelines, formats and standards.

Related Acquisition Cost Analysis and Estimation services are: Life Cycle Cost Estimating Service (SME005.1), Software Intensive Projects Cost Estimating Service (SME005.2) and Miscellaneous Cost Estimating & Analysis Service (SME005.4).

Value proposition: The Acquisition CA Service provides independent and unbiased price analysis for the provision of capability and/or system development projects and programmes. It offers full transparency and enables the Customers to verify whether the competitive price bids meet all the requirements of the bidding instructions and are ranked from low to high in terms of price. It supports the Customers in assessment and negotiations of the sole source proposals, as well as provides them with recommendations on the fairness and reasonableness of the prospective costs of the projects. By doing so, it empowers the Customers to make informed investment decisions. As a result, they are able to execute acquisition projects in an effective and efficient manner. Additionally, by providing negotiation support the Acquisition CA Service creates the opportunities for the Customers to achieve cost savings.

Service Features:

Competitive Bid Price Evaluations, ranking the bidders in terms of price, or to determine the price score for a Best Value competition;

Non-competitive Bid Price Evaluation, performed on sole source price proposals to determine if the proposed price is fair and reasonable;

Negotiation support: developing the Customer and Objective positions through independent cost estimates, project benchmarking and analysis of technical inputs and assessments.

Service Flavours:

Competitive Bid Price Evaluations (Best Value and Lowest Compliant Bid); Status: Available now;

Request for Quotation (RFQ) Pricing Support;

Bidding Sheets;

Price Evaluation incl. Report;

Non-competitive Bid Price Evaluations; Status: Available now;

Request for Quotation (RFQ) Pricing Support;

Bidding Sheets;

Price Evaluation incl. Report;

Negotiations support; Status: Available now;

Project benchmarking;

Providing supporting data and reports;

Attending in person.

Products and the enabling tools:

Product/Service	Tool/Method
SW projects benchmarking	FPA/ISBSG
Bidding sheets, Price Evaluation Report	MS Excel
Enterprise Information tool	EBA

Available on: No network security dependency/restrictions;

Service Prerequisites: Customers will be required to provide the following information to the cost estimating service including but not limited to:

Scope definition based on a clear set of requirements;

Schedule of Supplies and Services (3S) (if available) listing the contract Deliverables, the quantities required, the location and the date of delivery;

Statement of Work (SOW) (if available) with the specification of work to be done;

Work Package (WP) (if available) definition;

Acquisition method.

Standard Service Support Levels: N/A

Service Cost / Price: Acquisition Cost Analysis Service will be costed based on level of effort (LOE). The CA Service delivery cost will be charged in accordance with specifically arranged conditions for the delivery. The LOE is estimated based on the requirements and subject to Customer agreement.

SME005.4 Acquisition Miscellaneous Cost Estimating & Analysis (MCEA) Service

Service ID: SME005.4

Service Name: Acquisition Miscellaneous Cost Estimating & Analysis (MCEA) Service

Portfolio Group: Subject Matter Expertise Services

Service Description: The Acquisition Miscellaneous Cost Estimating & Analysis Service encompasses a range of supporting cost estimating and analysis activities next to the separately covered activities in Life Cycle Cost Estimating Service (SME005.1), Software Intensive Projects Cost Estimating Service (SME005.2) and Cost Analysis Service (SME005.3).

All products and activities performed within this Acquisition MCEA Service are in line with the NATO Costing Practices. They follow the best practice of the latest governmental guidelines, formats and standards.

Value proposition: The Acquisition MCEA Service supports the Customers by providing them with the whole range of supporting activities and products enhancing their ability to: acquire capabilities; monitor and manage projects and programmes.

Parametric Analysis (PA), predictive modelling, forecasting, simulation and optimization, support to Risk Management, support to Business cases together with What-if simulations enable the Customers to make informed investment decisions. Earned Value Management (EVM), audits, analysis of historical data and benchmarking help them keep track of the performance of their projects and stay in control.

Service Features: Miscellaneous: a whole range of analyses, models and activities to track and control project progress, generate savings, support negotiations, forecast and optimize costs.

Service Flavours:

Parametric Analysis (PA) including Cost Estimating Relationship (CER) Development;
Status: Available now;

Earned Value Management (EVM); Status: Available now;

Predictive modelling, forecasting, simulation, and optimization (Monte Carlo); Status:
Available now;

What-if simulations; Status: Available now;

Project/Contract audits; Status: Available now;

Claim evaluations; Status: Available now;

Support to Risk Management; Status: Available now;

Software projects benchmarking; Status: Available now;

Analysis of Historical Data; Status: Available now;

Support to Business Cases (BC); Status: Available now

Products and the enabling tools:

Product/Service	Tool/Method
SW projects benchmarking, Analysis of Historical Data	FPA/ISBSG
Predictive modelling, forecasting, simulation, and optimization, What-If Simulations, Monte-Carlo	Crystal Ball
Parametric Analysis, CER Development, Earned value Management	MS Excel
Parametric Models, What-If Simulations	SEER Suite
Option analysis and risk prioritisation	TOPSIS
Enterprise Information tool	EBA

Available on: No network security dependency/restrictions;

Service Prerequisites: Customers will be requested to provide the following information to the cost estimating service including but not limited to:

Scope definition based on a clear set of requirements;

Schedule of Supplies and Services (3S) (if available) listing the contract Deliverables, the quantities required, the location and the date of delivery;

Statement of Work (SOW) (if available) with the specification of work to be done;

Work Package (WP) (if available) definition;

Acquisition method.

Standard Service Support Levels: N/A

Service Cost / Price: Acquisition Miscellaneous Cost Estimating & Analysis Service will be costed based on level of effort (LOE). The Service delivery cost will be charged in accordance with specifically arranged conditions for the delivery. The LOE is estimated based on the requirements and subject to Customer agreement.

SME006 Operational Analysis Service

Service ID: SME006

Service Name: Operational Analysis Service

Portfolio Group: Subject Matter Expertise Service

Service Description: Operational Analysis (OA) is a consultancy service, which consists of developing and applying fit-for-purpose approaches and scientific methods to analyse problems across the spectrum of defence activities, and supporting decision makers in understanding, visualising and resolving them.

Value Proposition: The OA service helps decision makers within NATO and the Nations to make better informed decisions based on evidence. This service offers reliable and timely expert support to decision makers in NATO and Nations. Professional analysts, who have an excellent understanding and extensive experience in defence and security issues, supported by analytical supporting tools (e.g. models) and techniques (e.g. wargaming, data science), are able to help scoping an issue that decision makers face and provide objective analysis of available options, leading to better informed decision making. The OA experts have decades of involvement in defence planning support, OA support to Alliance Operations and Missions, and support to peacetime and operational Headquarters. They also have a proven track record of delivering high quality expertise and products to customers' satisfaction, on time and within budget.

Service Features: NCI Agency can provide ad hoc and flexible Operational Analysis consultancy to NATO and Nations through the application of tailored analytical methods to solve complex problems as typically faced by organisational leaders and operational commanders. The Service can provide support in a range of fields such as the following (non-exhaustive list). Of note, the support and techniques described here can also be applied in other context.

- **Defence Planning:** provision of a full spectrum of technical consultancy, analysis and advice to support NATO and the Nations in Defence Planning (DP), primarily with focus on support to the NATO Defence Planning Process (NDPP). It includes (non-exhaustive list):
    - Analytic expertise in support of the NATO Defence Planning Process (NDPP) activities, including identification of capability requirements, apportionment of requirements, and suitability and risk assessment; this analytic support involves for instance:
        - Development of new methodologies;
        - Analysis, including very large data sets, through a range of modelling techniques and tools;
        - Development of representative scenarios;
        - Structured mission analysis (mission-to-task decomposition);
        - Assessment of risk and aggregation techniques;
        - Support to assessing burden sharing in terms of relative costing techniques;
        - Application of OA techniques to facilitate decision making;

    - Provision of subject matter expertise (SME) across military and non-military domains, including reach to extensive networks of SMEs across NATO and in the nations;
  - Analytic expertise in support of national Defence Planning activities, such as:
    - Education and mentoring with NATO analytic approaches;
    - Facilitation and delivery of customised Defence Planning studies;
    - Access to and development of analytic supporting tools and models (e.g. the Joint Defence Planning Analysis and Requirements Toolset (JDARTS));
    - Support to implementation of robust national capability-based planning processes;
    - Exploitation of established NATO best practice, tailored to fit national needs;
    - Facilitation of the use of NATO DP tools & models.

- **Support to Headquarters (peacetime & operational):** provision of tailored analytical support to tactical, operational and strategic-level HQs within Nations and the NATO Command and Force Structures, during peacetime and/or crisis situations. This support includes areas such as:

  - Wargame development and facilitation;
  - Support to planning activities such as Course of Action analysis, support to concept development activities, lessons identified;
  - Operational assessment, battle information management, data analysis (time-series, geospatial, survey), and streamlining of existing HQ data collection/analysis processes, implementation of advanced analytical techniques (mathematical modelling and optimisation algorithms);
  - Organisational design and improvement of processes, including analysis of ‘as-is’ processes and provision of ‘to be’ structures or changes;
  - Support to analysis of information exchange requirements, and modelling of processes and information flows.

  This support is available on-site (static or deployed locations) or as remote, reach back arrangement.
- **Operational and User Requirements:** provision of expertise to support, through exploitation of products and knowledge from any of the other OA services, a range of areas including:

  - User requirements capture and validation;
  - Mentoring in the employment of NATO Functional Area Services (FAS) to meet military business process and information exchange requirements;
  - Business decision support e.g. development of NATO FAS Lifecycle Roadmap;
  - IT procurement and training decision support e.g. development of dashboard highlighting technology employment/retirement and deprecation;
  - Gap analysis to enable the integration of NATO processes to ensure a seamless "end-to-end" approach to capability delivery and sustainment.
  - Support to architecture development.

Service Flavours: The OA service is tailored to meet individual needs of a customer.

Available on: N/A

Service Prerequisites:

None

Standard Service Support Levels: N/A

Service Cost/ Price: The unit of measure for the Service is Per Defined Service. Cost for each defined service is individually set up, in accordance with agreed scope and conditions of the service delivery, as well as valid NCI Agency Customer Rates.

SME007 Operational Application Support Service

Service ID: SME007

Service Name: Operational Application Support Service

Portfolio Group: Subject Matter Expertise Service

Service Description: Operational Application Support Service maintains and supports a consistent and interoperable FAS set up for External Customers stakeholders. It provides technical support for the FASes including:

- JCHAT, MLINK, OPENFIRE, JOCWATCH, LOGFAS, TOPFAS-EFGTM/NCRS/RRT/OCC
- NIRIS, NISP, ICC, JTS/FAST, SEW, AIRC2IS, MCCIS
- NCOP, LC2IS
- INTEL-FS, HMART, NAMIS, CORE GIS

Value Proposition: This flavour ensures External Customers' operational support requirements are addressed for effective use of NATO FASes to enable their preparedness for missions.

Flavour includes access to Incident Management Tool (ITSM), management of trouble tickets, and Centralised Service Desk support for initial response.

Service Features:

- Support for Incidents and Service request[1]
- Problem management
- Monitoring and Event management (if agreed with a Customer and remote access is possible)
- Software upgrades in line with the NCI Agency approved FAS (COI) baseline. It includes:
  - Up to one onsite supported upgrade
  - Up to two remotely supported upgrades of the existing installed FAS (COI) instances (e.g. through emails, ITSM, remote access, and phone)

The scope is a subject of annual refinement, as new applications and versions integrate into NATO FAS (COI) baseline, or old applications become obsolete and out of support.

Escalation criteria and timelines, e.g. Time to Response and Time to Resolve, are defined as part of the reference framework. The details usually relates to SSP, but also can be negotiated.

By default, the on-site installation is limited to one service instance per FAS (COI) application. Additional instances are subject to resource availability (work force, time, funds).

[1] *In the case NCI Agency has no remote access (connectivity) to the National application services supported, NCI Agency will provide remote support in the form of guidance in troubleshooting and resolution. Guidance for resolution will include a proposed solution within the agreed timeframe.*

Change requests to the application deliverables that trigger source code modification are, however, not part of this Service

Service Flavours:

1. **Bundle B** - Support to JCHAT, MLINK, OPENFIRE, JOCWATCH, LOGFAS, TOPFAS-EFGTM/ NCRS/RRT/OCC
2. **Bundle C** - Support to NIRIS, NISP, ICC, JTS/FAST, SEW, AIRC2IS, and MCCIS
3. **Bundle D** - Support to NCOP, LC2IS
4. **Bundle E** - Support to INTEL-FS, HMART, NAMIS, CORE GIS

Following options can be requested additionally:

On-site support – Available for each bundle, service cost table depicts the additional cost per each bundle.

Complete Solution – Includes remote and on-site support for all listed applications (all bundles).

Tailored FAS (COI) OPS Scale: The Service conditions adopted to meet specific customer requirements (e.g. changed or reduced number of supported applications or adjusted scope of support) per site, per bundle.

Extended FAS (COI) OPS: Support required outside of normal business hours per site, per bundle, on weekends and public holidays; additional charges apply.

Available on: Any network of customer subject to security requirements.

Service Prerequisites: Minimum of one functional FAS (COI) application on the site requiring the Service.

Standard Service Support Levels:

Service Availability: The service is available during standard business hours.

Ticket can be raised 24/7 however support availability is:

Availability Target
Business Hours **Mon-Fri 08:30 – 17:30 CET**

Service Restoration: Not applicable.

Service Cost / Price: For the flavours/options where there is a defined unit of measure, a standard service cost is specified. For the Extended FAS (COI) OPS and Tailored FAS (COI) OPS Reduced Scale options, the unit of measure is 1, the total of the service delivery cost for these flavours is charged in accordance with specifically arranged conditions of the service delivery.

Service Flavours / Service Options	Service Unit
Regular FAS OPS - Bundle B	Per Site
Regular FAS OPS - Bundle C	Per Site
Regular FAS OPS - Bundle D	Per Site
Regular FAS OPS - Bundle E	Per Site
Regular FAS OPS - On-Site Support Option	Per Site/Per Bundle
Regular FAS OPS - Complete	Per Site
Extended FAS OPS	1 (custom calculated)
Tailored Reduced FAS OPS	1 (custom calculated)

SME008 Maritime Operational CIS Deployment and Recovery Service

Service Name: Maritime Operational CIS Deployment and Recovery Service

Portfolio Group: Subject Matter Expertise Services

Service Description: This service provides delivery, installation, configuration, commissioning, and when required, subsequent decommissioning and removal of CIS services. These services may include all or some of the following; Maritime Command and Control Platform (MARC2P) Service (PLT012), SEMARCOM/SEMARCIS service (INF044), Tactical Satellite (TACSAT) service (INF040), and the NATO Control and Reporting Centre (CRC) System Interface (CSI) service (INF041). These services can be provided to and from customer designated location(s) within SACEUR's Joint Operational Area (JOA).

Value proposition: This service enables the customer to maintain a level of operational command and control when established on board a designated vessel or at a specified static location.

Service Features:

Planning: This requires in depth coordination with the customer, any nominated additional points of contact, the designated Naval vessel, and if necessary, the Host Nation (HN) of the oncoming vessel. The planning process also includes a site survey of the oncoming vessel 90 days ahead of time for full operational handovers. A site survey may be required for all other activities. This is critical to facilitate a common understanding of the full scope of the upcoming activity, and to advise the HN designated vessel in their preparation to take on the CIS services.

Deployment: Includes the requested CIS service(s) equipment to be forward deployed to a designated Naval vessel (or static location) for installation.

Implementation: Includes the installation, configuration, and commissioning of requested CIS service(s). Equipment is installed on the identified Naval vessel (or static location), and End-to-End (E2E) configuration is completed utilizing remote support from various NCI Agency service areas. All CIS Services are tested on site and commissioned when considered operational and agreed with the customer on site.

Training: Training is provided on site during implementation to designated staff. This includes operator and basic administrator training to facilitate a common understanding of CIS operations, standard operating procedures (SOPs), and basic troubleshooting.

Recovery: Where requested, CIS service(s) equipment will be decommissioned (ceasing services), de-installed, and then subsequently recovered to NCI Agency control. At times the same equipment may be immediately re-allocated for additional tasking.

Service Flavours:

SME008-1 Maritime Operational CIS Deployment/Recovery Service – Collocated Major Handover: Includes removal of the SNFC2P, TACSAT (if installed), and/or SEMARCIS/SEMARCOM (if installed) CIS equipment from one identified Naval vessel, immediately followed by installation on another identified Naval vessel at the same designated port of call.

SME008-2 Maritime Operational CIS Deployment/Recovery Service – Non-Collocated Major Handover: Includes removal of the SNFC2P, TACSAT (if installed), and/or SEMARCIS/SEMARCOM (if installed) CIS equipment from one identified Naval vessel at one designated location, shipment of CIS equipment (via Northwood if required), and subsequent additional travel to a different location for installation on another identified Naval vessel at that separate location.

SME008-3 Maritime Operational CIS Deployment/Recovery Service – NATO Control and Reporting Centre (CRC) System Interface (CSI) Deployment / Recovery (DR): Includes deployment and implementation of a CSI capability on an identified vessel at a designated location and then subsequent recovery of the CSI equipment from that vessel at a later date and designated location (may be the same or different from the installation location).

SME008-4 Maritime Operational CIS Deployment/Recovery Service – SEMARCIS / SEMARCOM Deployment / Recovery (DR): Includes deployment and implementation of a SEMARCIS or SEMARCOM capability on an identified vessel at a designated location and then the subsequent recovery of the SEMARCIS or SEMARCOM equipment from that vessel at a later date and designated location (may be the same or different from the installation location).

SME008-5 Maritime Operational CIS Deployment/Recovery Service – Tactical Satellite (TACSAT) Deployment / Recovery (DR): Includes deployment and implementation of a TACSAT capability on an identified vessel at a designated location and then the subsequent recovery of the TACSAT equipment from that vessel at a later date and designated location (may be the same or different from the installation location).

Available on:

NATO Secret
Mission Secret
NATO UnclassifiedNon-Secure

Service prerequisites:

All service requests must be funded prior to deployment and implementation. This may include support provided under an existing agreement (SLA/SSP) or through funding via the Customer Request (CRF) process.

It is the Customer's responsibility to ensure compliance with the Minimum Military Requirements (MMR) for CIS as stipulated in the MC0195 prior to implementation. The customer is to ensure that the identified Naval vessel has the technical capabilities to support the CIS services (i.e. sufficient bandwidth, National connectivity, authority to install and/or connect to National systems, etc.).

An IT Service Request (ITSM) Change Request Form (CRQ) is required for each requested activity and must include all tasking requirements, POCs, dates and location(s). CRQs are submitted per the schedule below. In exceptional circumstances, this may be shorter, but this will require the customer to accept additional risk of the operational capability of their identified vessels.

- For SME008-1 and for SME008-2 a CRQ is required 120 days prior to date of handover.
- For SME008-3/4/5 a CRQ is required 30 days prior to date of activity.

The Customer is to facilitate agreed support for NCIA with the identified Naval vessels at agreed dates and location for implementation. This includes access to the base location, the Naval vessel(s) and coordinating local support on site (i.e. service crane, HN ship support).

A Customer Staff POC is requested to accompany the CSU team onsite during any installation activity.

The Customer is responsible for accepting and maintaining accountability of all CIS hardware after implementation until they are formally recovered by NCIA.

The Customer is responsible for ensuring the provision of cryptographic material in order to enable secure communications during operation of the deployed CIS, after implementation.

Delivery of this service is dependent on allocation of CIS equipment from designated account holders or the customer holding these resources. It is the Customer’s responsibility to ensure that the requested resource is available.

Standard Service support levels*:*

The Service is available at any point in the calendar year.

There is a maximum concurrency of two Deployment / Recovery activities at any time to include travel to/from locations. Any additional concurrent requests will only be considered by exception and on a case by case basis manner.

Service Cost / Price: The unit of measure for the Service is per instance of service flavour requested. For price information, see the Service Rates document.

Service Performance Targets:

Implementation completed by required date for Service Change Requests received with sufficient notice (timelines specified above) and meeting all prerequisites: 95%

Time to complete:

SME008-1. 4 days total.

SME008-2. 5 days total: 4 days for implementation; 1 day for recovery.

SME008-3. 3 days total: 2 days for implementation; 1 day for recovery.

SME008-4. 3 days total: 2 days for implementation; 1 day for recovery.

SME008-5. 3 days total: 2 days for implementation; 1 day for recovery.

SME009 Provision of Subject Matter Expertise to support NCS as an Affiliate to Federated Mission Networking (FMN)

Service ID: SME009

Service Name: Provision of Subject Matter Expertise to support the NCS as an Affiliate (NCSaaA) to the Federated Mission Networking (FMN) Initiative.

Portfolio Group: Subject Matter Expertise Services

Service Description: The scope of this service is to provide subject matter expertise services to Allied Command Operations (ACO) in order for the NATO Command Structure (NCS) to contribute as an Affiliate and conduct activities to maintain the Federated Mission Networking (FMN) Framework.

Value Proposition: With NAC approval of NFIP Vol 1 on 29 January 2015 (C-M(2015)0003-AS1), the NCS itself is committed to participate as an Affiliate to the FMN Initiative and therefore need to contribute to the maintenance of the FMN Framework (the roles of the NATO entities to enable the NCS to participate within FMN is described in MC0660, dated 15 January 2018). This service is to maintain ACO's portion of the NATO funded support to enable the NCSaaA to take part in the FMN framework. The maintenance of ACT's portion of the NATO funded support to enable the NCSaaA to take part in the FMN framework is funded via the ACT POW.

Service Features: The Service provides the following areas of expertise and facilities:

- **Support the Management of the NCSaaA.**
  - Provide SME to support ACOS J6 within his role as NCS Affiliate Representative within the FMN Management Group (MG);
  - Provision of Technical Advice in support of NCSaaA routine preparation for Military Committee Working Group (CIS) (MCWG (CIS)) meetings prior to FMN MG and FMN MG Preparation meetings.
- **Represent the NCSaaA in FMN Architecture related activities.**
  - Provision of an enterprise architect to represent NCSaaA in the Architecture Coordination Board (ACB) and to follow up on decisions and actions.
- **Support the Representation of NCSaaA within the FMN Operational Coordination Working Group (OCWG).**
  - Provision of an operational analyst to support the derivation and maintenance of NCS Affiliate Operational Requirements for inclusion within the FMN Operational Requirements process.
- **Support the Representation of NCSaaA within the FMN Coalition Interoperability, Assurance and Validation (CIAV) Working Group.**
  - Represent NCS Affiliate as the National lead within FMN CIAV;
  - Provide NCS Affiliate CIAV Support to FMN Integrated Working Groups (IWG) and ACB;
  - Represent NCS Affiliate in FMN CIAV WG Break Outs and meetings;
  - Plan and execute AV&V Events to support NCS Affiliate requirements (i.e. conduct AV&V for each NCSaaA Request for Change to enable inclusion in FMN baseline);

  - Provide CV2E lab support.
- **Support the Representation of NCSaaA within the FMN Change and Implementation Coordination Working Group.**
  - Provision of a Service Engineer to prepare and manage NCSaaA Requests for Change (RFC) to the FMN Product Baseline.
- **Support the annual technical assessment of federation at Exercise STEADFAST COBALT (STCO).**
  - Provision of a Service Engineer (with a broad technical knowledge of federation) to the JFC led evaluation team.
- **Travel**. Due to the meeting schedule of the FMN initiative and its working groups, there is considerable Travel associated with this service.

Service Request: The service can only be requested as follows:

- ACO funded: via the CSLA (SLIN13.1 and Activity 525);

Service Flavours: The service comes as a complete package and is originally based on the scope of ACO funded tasks and funding levels described in 6300/TSC-FCX-0010/TT-140441/Ser:NU1023 dated 7 NOV 14. Over the intervening years this has evolved to keep pace with demand and NCSaaA tasks have been split out from SME004 into SME009.

Available on: The SME can provide services/advice through the following networks:

- Support to ACO, ACT and NHQC3S that support the direction and development of the FMN Framework for the NCSaaA: Unclassified (NU DNBL NRF MN Gov & Mgt Portal)/NR (Advice)/NS (NS DNBL NRF MN Gov & Mgt Portal)
- Support to derisking of the implementation of federated capabilities through collective and federated CIAV testing with other Affiliate Nations: Unclassified (DNBL CIAV Portal)/NR (Advice)/NS (Advice)/CV2E (federated CIAV laboratory)..

Service prerequisites: N/A

Standard Service Support Levels*:* N/A

Available/Related NCI Academy Training not covered by service cost:

A0104	NATO CIS Planning

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery. The service charge should take into account the extensive TDY commitment.

SME010 ACP127 Message Operator Service

Service ID: SME010

Service Name: ACP127 Message Operator Service

Portfolio Group: Subject Matter Expertise Service

Service Description: This service provides 24/7 ACP127 Message Operator Support to NCI Agency External Customers in cases where their own nations are not providing them with adequately integrated ACP127 Military Message Operator services.

Value proposition: The ACP127 Message Operator Service provides to NCI Agency External Customers, efficient organisational access to and inclusion in, formal command-to-command communication with other entities in the NATO Command Structure, NATO Force Structure, NATO Nations, Missions environments, and Multinational Organisations. This 24/7 service includes manual assistance with the release and distribution of messages which have failed automatic processing, the forwarding of messages to mobile units which have been misaddressed, and the reporting of problems which affect timely delivery of formal messages.

Service Features:

ACP127 Signal Message Addressee (SMA): An organizational SMA will be created and a routing indicator will be assigned. The information (including Long Title and Location) will be appropriately published. The SMA will then be available for integration into AIGs or other collective addresses.
Note: The term SMA is used interchangeably with Plain Language Addressee, or PLA or PLAd.

Organisational Receipt of ACP127 Messages: Messages addressed to the SMA are received by the Communications Centre (*Commcen*) and distributed by email to pre-arranged NSWAN-reachable Functional mailboxes. Indirect relay over NATO Mail Exchanges will be used whenever direct SMTP email service is not made available. Nightly reports permit independent verification of the previous day's message distribution.

Organisational Sending of ACP127 Messages (optional): Origination of and reply to ACP127 Messages requires installation and maintenance by local technical support team of the AIFS Integrated Message System (AIMS) software and maintenance of a coordinated authorised releaser list. The Commcen confirms each AIMS release with a Release Notification receipt.

ACP127 Organisational Support: Messages which fail automatic processing are handled 24/7. Upon request, the Message Service Operator can re-distribute messages, retrieve messages, or trace delivery and receipt of messages. Release and distribution rules are adapted as required.

ACP127 Message Handling: ACP127 messages are transmitted according to precedence, enforcing flash receipt and ensured end-to-end delivery (fire-and-forget). Exceptionally, any messages which cannot be delivered will be "serviced" back to originating Commcen. If necessary ACP127 Messages can be traced from end-to-end throughout the entire store and forward ACP127 Military Messaging network. The

Commcen regularly maintains addressing databases to provide accurate addressing and delivery.

Service Flavours: The service is available as a single flavour.

Available on:

NATO Secret

Service prerequisites:

INF002 - NATO Network Point of Presence

Standard Service support levels:

Service Availability Target: 99.0%

Service Restoration: Where the service is deemed unavailable, the service restoration period is 8 hours. However, this presumes that all underlying services provided by the nation are available (including but not limited to NSWAN connectivity, routers, firewalls, Exchange servers, etc.). Messages will be held in the Commcen until delivery is available.

Available NCI Academy Training not covered by service cost:

A0161	Allied Information Flow System (AIFS) Operator/Shift Supervisor
A0600	AIFS Pre-study (106)

Service Cost: The unit of measure for the Service is per Signal Message Address (SMA). Price Details available in the Service Rates document.

SME011 Subject Matter Expertise and Technical Consultancy Service for NATO Software Tools (NST) Communications and Information (C&I) Partnership

Service ID: SME011

Service Name: SME and Technical Consultancy Service for NST C&IP

Portfolio Group: Subject Matter Expertise Services

Service Description: NST C&IP provides Participants with SME and Technical Consultancy services for evolution of programme of work including incorporation of new operational requirements, building and/or acquiring new tools, collection and management of NST C&IP related functional service and support requirements for subsequent years' Programme of Work.

Based on this service provision for participant Nations, NST C&IP is experienced to advise requestors, primarily the potentially joining Nations, on the best use of a wide range of NCI Agency services related to applications, to meet their specific business requirements and achieve their business objectives (See service features).

Value Proposition: For provision of these services, NST C&IP POW leverages on the experience and accumulated knowledge of NST C&IP and other NCI Agency teams supporting NATO Nations and organizations to align with the NATO technological vision and NCI Agency processes.

NST C&IP core team evaluates the service request and provides support on NCI Agency processes, legal, contractual and IPR issues of NATO FASes usage for national purposes. If the service request is related to the applications and business processes themselves, SMEs of specific systems and processes are involved. If the service request is related to infrastructure, request is forwarded to teams with in-depth knowledge on infrastructure.

Service Features:

- Provision of remote SME support on NCI Agency processes

  1.1 SME support for Request for Information(RFIs) on NCI Agency processes such as acquiring access to EDML, joining a partnership, and submitting a CRF.

- Provision of remote SME support on legal, contractual and IPR issues and constraints with utilization of NATO FASes for national purposes

  2.1 SME support for RFIs on current status and initial analysis towards the resolution of issues

- Integration of C5ISR[1] IT systems related to NATO FASes

[1] Command, Control, Communications, Computers, Combat Systems, Intelligence, Surveillance, and Reconnaissance

3.1 Remote SME support for RFIs on new solutions and their feasibility and cost analysis for way ahead

- Achievement of increased effectiveness in usage of NATO FASes to manage business processes

4.1 NST C&IP FAS Overview training on-site
4.2 On-site SME support for implementing national processes via the usage of NATO FASes
4.3 Provision of initial feasibility and cost analysis for business process interoperability between NATO and national tools
4.4 On-site SME support for RFIs on new business solutions and their feasibility and cost analysis

- Resolution of infrastructure and NATO/Nation network boundaries issues and architectural changes affecting workability with NATO FASes

5.1 Provision of one service request for changing the existing network configuration
5.2 Provision of remote SME support for addressing potential solutions and cost estimates for wider service request

- NATO FASes application lifecycle transformation including the adoption of current and new technology, methodologies and processes such as DevOps[1], Microservices[2], Containerization[3] and Cloud Technologies[4]

6.1 Provision of on site knowledge transfer session on new technologies:
6.2 Remote SME Support for effective usage of new technologies within the Nation:

  - Determination of strategy for the way ahead
  - Stakeholders analysis

- Inclusion of national requirements in NATO Applications in the NST C&IP POW toolset mainly via the provision of support for:

7.1 Requestor representatives in Change Control Boards (CCBs) and Operational User Groups (OUGs)
7.2 Formulation of one user requirement or change request for inclusion

[1] DevOps is a culture that promotes collaboration between Development and Operations Team, which allows deploying code to production faster, and in an automated way.

[2] Microservices are a software development technique—a variant of the service-oriented architecture (SOA) architectural style that structures an application as a collection of loosely coupled services.

[3] Container is a standardized unit of software which isolate component from its environment and ensure that it works uniformly despite differences for instance between development and staging. NST C&IP provides containerization support to develop a common understanding of containerisation strategy and to analyse how best to exploit containerisation for the NATO FASes.

[4] Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user.

7.3 End-to-end monitoring and reporting on the change management processes

Service Flavours:

Remote support - Available
On-site support – Available

Available on: Any network of customer subject to security requirements of specific FAS application

Service Prerequisites: None

Standard Service Support Levels*:*

Service Availability: *The service is available during standard business hours.*

Ticket can be raised via NST C&IP Inbox 24/7 however the NST C&IP Support availability is:

Availability Target
Business Hours Mon-Fri 08:30 – 17:30

Service Restoration: N/A

Service Cost / Price: Cost for each defined effort is individually calculated, in accordance with agreed scope and conditions of the service delivery, as well as valid NCI Agency Customer Rates.

References:

- NST C&IP 2020 POW and Appendices
- CIP General Rules, 08 Dec 2015
- NST CIP Partnership Arrangement, 12 Oct 2016

SME012 VeVA CIAV Support

Service ID: SME012

Service Name: VeVA CIAV Support

Portfolio Group: Subject Matter Expertise Services

Service Description: The Vigilance and enhanced Vigilance Activities (VeVA) Coalition Interoperability Assurance and Validation (CIAV) support is comprised of the following packages:

1. VeVA Governance and Management Support
2. Interoperability Verification and Validation – Foundation package + Year Round support for VeVA
3. Interoperability Verification and Validation – Steadfast Cobalt Exercise
    - a. Scope Parameters:
        - i. Up to 3 test scenarios
        - ii. Up to 50 participants
        - iii. Participation on four planning conferences of 5 days
        - iv. Participation on SMA conference, IER workshop, academics and ESC conference of 4 days each
        - v. Lead and participate three test management workshops of 5 days each
        - vi. Services in scope : Up to 35 Services
        - vii. Execution timelines: 3 weeks for Phase IIIA (Federation Joining V&V) and 4 weeks for Phase IIIB (Federation V&V)
    - b. The service description and costing is valid for the event parameters as described above. Any change in those parameters must be complemented by a relevant Customer Request Form specifying the scope and associated funding, subject to a dedicated project covering requested activities.
4. Interoperability Verification and Validation – Joining/Exiting Event for VeVA
    - a. Scope Parameters:
        - i. Up to 1 test scenarios
        - ii. Up to 15 participants
        - iii. Participation on one planning conferences of 5 days
        - iv. Lead and participate one test management workshops of 5 days
        - v. Services in scope : Up to 35 Services
        - vi. Execution timelines: 2 weeks
        - vii. Note: It is planned to be executed quaterly, except when Steadfast Cobalt event is in execution
    - b. The service description and costing is valid for the event parameters as described above. Any change in those parameters must be complemented by a relevant Customer Request Form specifying the scope and associated funding, subject to a dedicated project covering requested activities.
5. Interoperability Verification and Validation – Change Management Event for VeVA
    - a. Scope Parameters:
        - i. Up to 1 test scenarios
        - ii. Up to 10 participants
        - iii. Participation on one planning conferences of 3 days each

iv. Lead and participate one test management workshops of 3 days each
v. Services in scope : Up to 15 Services
vi. Execution timelines: 1 week
vii. Note: It is planned to be executed monthly, except when Steadfast Cobalt event is in execution

b. The service description and costing is valid for the event parameters as described above. Any change in those parameters must be complemented by a relevant Customer Request Form specifying the scope and associated funding, subject to a dedicated project covering requested activities.

Value Proposition:

Service Features and Value proposition:

1. VeVA Governance and Management Support

   This service will provide CIAV support to the VeVA Governance and Management Structure. The following activities are covered:

   - CIAV WG Support
   - Coordination of VeVA MN CIAV WG with other WG of the Governance and Management Structure, providing testing guidance and support to other WG

2. Interoperability Verification and Validation – Foundation package + Year Round support for VeVA

   This foundation service will provide the VeVA access to the IO Toolset, the process and the most up to date verification and validation content ready to be used in the IO Toolset. Activities under this service are:

   - Support and guide VeVA in the way to test, verify and validate NRF interoperability and mission network federation
   - Review interoperability FMN requirements and IERs, as well as their specification and testability
   - Maintenance of High Level Verification and Validation Plan that will cover capabilities that are added, removed, or modified in the VeVA MN .
   - Maintenance of the VeVA instance of the IO Toolset, including the necessary processes to be able to run it in classified environments.
   - Maintenance of the content, always keeping the most up to date version of the repository.
   - Updates to non-FMN services content.

3. Interoperability Verification and Validation– Exercise Steadfast Cobalt

   a. Planning Package

   This on-demand service provides manpower support for performing V&V planning under the conditions specified under the scope parameters. This will provide the minimal CIS planning support that will enable verification and validation. It will also provide the customer with a detailed verification and validation plan to assure the

service design and implementation can be verified and validated. Furthermore, all the test executions are planned in the IO Toolset, ready to be executed.
Same activities (with different scope depending on the event) will be executed. Recurring activities are:

- Review and provide input to Test Procedures
- Review and provide input to Test Environment
- Provide training to participants on the process, the content and the toolset.
- Provide detailed event plan in the toolset including support to asset management.
- Provide individual test plans per participant.
- Schedule detailed test executions.

b. Execution and Reporting package
This on-demand service will provide manpower support under the conditions specified under the scope parameters for directing the execution by also implementing a complete testing organization which will lead the overall execution of all the tests. For each event, VeVA will get assigned a complete Event Team consisting of Interoperability Director, required Test Management Team and one or more Test Directors. After the event, all the results will be fully analysed and Technical Interoperability assessment will be provided to the VeVA MN Executive Group. The reporting service also provides the option for an evaluation team to create, update, manage and assess VeVA mission based on training objectives and evaluation criteria throughout the event.
Same activities (with different scope depending on the event) will be executed. Recurring activities are:

- Provide training to participants on the process, the content and the toolset.
- Guide the technical readiness self-assessment of the participants during service V&V for those required
- Direct the execution of federation joining V&V and federation V&V of the participants for those required.
- Provide verification and validation toolset and required support during the event
- Provide Report from the event.
- Provide lessons learned, process improvement, optimization

4. Interoperability Verification and Validation – Joining/Exiting Event for VeVA
   a. Planning Package
   This on-demand service provides manpower support for performing V&V planning under the conditions specified under the scope parameters. This will provide the minimal CIS planning support that will enable verification and validation. It will also provide the customer with a detailed verification and validation plan to assure the service design and implementation can be verified and validated. Furthermore, all the test executions are planned in the IO Toolset, ready to be executed.

Same activities (with different scope depending on the event) will be executed. Recurring activities are:

- Review and provide input to Test Procedures
- Review and provide input to Test Environment
- Provide training to participants on the process, the content and the toolset.
- Provide detailed event plan in the toolset including support to asset management.
- Provide individual test plans per participant.
- Schedule detailed test executions.

b. Execution and Reporting package

This on-demand service will provide manpower support under the conditions specified under the scope parameters for directing the execution by also implementing a complete testing organization which will lead the overall execution of all the tests. For each event, VeVA will get assigned a complete Event Team consisting of Interoperability Director, required Test Management Team and one or more Test Directors. After the event, all the results will be fully analysed and Technical Interoperability assessment will be provided to the VeVA MN Executive Group. The reporting service also provides the option for an evaluation team to create, update, manage and assess VeVA mission based on training objectives and evaluation criteria throughout the event.

Same activities (with different scope depending on the event) will be executed. Recurring activities are:

- Provide training to participants on the process, the content and the toolset.
- Guide the technical readiness self-assessment of the participants during service V&V for those required
- Direct the execution of federation joining V&V and federation V&V of the participants for those required.
- Provide verification and validation toolset and required support during the event
- Provide Report from the event.
- Provide lessons learned, process improvement, optimization

5. Interoperability Verification and Validation – Change Management Event for VeVA

a. Planning Package

b. Planning Package

This on-demand service provides manpower support for performing V&V planning under the conditions specified under the scope parameters. This will provide the minimal CIS planning support that will enable verification and validation. It will also provide the customer with a detailed verification and validation plan to assure the service design and implementation can be verified and validated. Furthermore, all the test executions are planned in the IO Toolset, ready to be executed.

Same activities (with different scope depending on the event) will be executed. Recurring activities are:

- Review and provide input to Test Procedures
- Review and provide input to Test Environment
- Provide training to participants on the process, the content and the toolset.
- Provide detailed event plan in the toolset including support to asset management.
- Provide individual test plans per participant.
- Schedule detailed test executions.

c. Execution and Reporting package

This on-demand service will provide manpower support under the conditions specified under the scope parameters for directing the execution by also implementing a complete testing organization which will lead the overall execution of all the tests. For each event, VeVa will get assigned an Event Team whose composition will vary according to the event scope. After the event, all the results will be fully analysed and Technical Interoperability assessment will be provided to the VeVa MN Executive Group.

Same activities (with different scope depending on the event) will be executed. Recurring activities are:

- Provide training to participants on the process, the content and the toolset.
- Guide the technical readiness self-assessment of the participants during service V&V for those required
- Direct the execution of federation joining V&V and federation V&V of the participants for those required.
- Provide verification and validation toolset and required support during the event
- Provide Report from the event.
- Provide lessons learned, process improvement, optimization

Service Flavours: The Service is available in various flavours:

Fixed packaging delivering:

- VeVA Governance and Management Support
- Interoperability Verification and Validation – Foundation package + Year Round support for VeVA
- Interoperability Verification and Validation – Steadfast Cobalt Exercise
- Interoperability Verification and Validation – Joining/Exiting Event for VeVA
- Interoperability Verification and Validation – Change Management Event for VeVA

Available on:

NATO Secret
Mission Secret

Service Prerequisites: N/A

Standard Service Support Levels: N/A

Service Cost / Price: Service cost is specified for the fixed package and each of the optional offerings. The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SME013 Single European Sky Air Traffic Management Research (SESAR) Capability Implementation Study

Service ID: SME013

Service Name: SESAR Capability Implementation Study

Portfolio Group: Subject Matter Expertise Service

Service Description: This Service utilizes NCI Agency Subject Matter Expertise (SME) to identify the impact of the Single European Sky (SES) initiative on the AirC2 systems used in NATINAMDS, to analyse, identify, validate solutions and identify to which extend and by when the AirC2 systems under the AirC2 Governance will have to be adapted.

The Single European Sky (SES) is an initiative launched by the European Commission (EC) to reform the architecture of European Air Traffic Management (ATM). The key objectives of SES are to restructure the European Airspace as a function of air traffic flows, to create additional capacity and to increase the overall efficiency of the ATM system. The SESAR programme is the “technical pillar” to achieve the SES objectives by modernising the ATM of civil aviation in Europe. The SESAR Deployment Programme (DP) has introduced new concepts resulting from the SESAR research.

In 2016 and 2018, ACT conducted two initial studies, which focused on possible improvements to ACCS to cope with upgrades introduced by SESAR 1 Research Programme (2008-2016).

These studies will continue into identification and validation of requirements for upgrading NATO and National AirC2 Systems to remain interoperable with ATM and Air Traffic Control (ATC).

Value Proposition: This service combines NCI Agency SME holding AirC2 system expertise with information and background information available through liaison with EUROCONTROL as necessary to identify and validate the impact of SESAR on the NATINAMDS.

Service Features: This expert matter Expertise Service will complete the studies, analyse the SESAR DP and timelines, analyse and identify potential impact from SESAR, develop, prototype and validate potential solutions and propose change requests for affected AirC2 systems together with a necessary implementation timeline or roadmap.

The service is aimed at advising SHAPE as the main customer and the AirC2 governance on required action, priorities and timelines to stay compatible ATM/ATC when SESAR will be rolled out.

Service Request: Service should be requested through a CRF, or by a SLA/POW

Service Flavours: The service is provided as a singleton service through the AMDC2 ISS POW.

Available on: N/A

Service Prerequisites: N/A

Standard Service Support Levels*:* N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions between NCIA and SHAPE on an annual basis via AMDC2 ISS POW.

SME014 Provision of SME to support the Governance and Management of the VeVA Mission Network

Service ID: SME014

Service Name: Provision of Subject Matter Expertise (SME) to support the Governance and Management of the Vigilance and Enhanced Vigilance Mission Network (VeVA MN)

Portfolio Group: Subject Matter Expertise Services

Service Description: The scope of this service is to provide subject matter expertise services to Allied Command Operations (ACO) to enable NCI Agency to fulfil its roles in the multinational VeVA Governance and Management structures, support the processes and provide the required facilities. As the Service Management Authority (SMA) for the VeVA MN, the NCI Agency has a key role in supporting Supreme Allied Commander Europe (SACEUR) in the exercising of Command and Control (C2) over forces assigned by Nations for the execution of the Family of Plans (FoP) for the Defence and Deterrence of the Euro-Atlantic Area (DDA) and the Allied Response Force (ARF), when acting as SACEUR's strategic reserve.

Value Proposition: NAC approval of NFIP Vol 1 on 29 January 2015 (C-M(2015)0003-AS1), established that each Mission Network established would require a single service management authority (SMA), so that each mission network would operate under a single, centralized management model. In line with its existing technical authority role under the C2 arrangements (SH/CCD J6/PT A/27 4/15-31 0233), NCI Agency is appointed as the SMA for MN federations supporting NATO-led operations or missions (MC0660, ACO Directive 80-96). This includes the VeVA MN that is being established to support the Family of Plans for the Deterrence and Defence of the Euro-Atlantic Area (DDA FoP). The duties of the VeVA MN SMA and the descriptions of the other authorities and working groups and boards in which NCI Agency staff either are expected to lead and/or support are described in the ACO directive for the Governance and Management of the VeVA MN (SH/CYBER J6 Cy/SPP/ xx/xx/xxxxx currently SHAPE-Tasker-016449).

Context: This service operates within the context of the support provided by NCI Agency for Operations and Exercises, Independent Verification and Validation (IV&V) and Service Management and Control (SMC):

- Service SME014 was originally created to support the SMA of the NATO Response Force Mission Network (NRF MN). The planned resource level for the NRF MN SMA resides in SLIN10 of the central SLA (cSLA). Given that the NRF MN is superseded by the VeVA MN in 2024 and given that the VeVA MN is of a different scale and nature to the NRF MN, SME014 as a service has been transformed to satisfy the new requirement.
- IV&V support for VeVA MN CIAV WG meetings is handled in SLIN11 as SME012. SME012 is constructed using the same assumptions and parameters as SME014 regarding the nature of VeVA MN.

- The VeVA MN CIS OPCEN is in the process of being defined. Its role in the management of the VeVA MN and the associated NCI Agency resource requirements is anticipated to be defined as a separate service or added to an existing service.

Service Features: NCI Agency support to VeVA MN Governance and Management is comprised of the following packages that are scaled as follows:

- Support Routine VeVA MN Governance and Management. This is a foundation package providing year round support for VeVA MN Governance and Management and routine change management.
    - Scope parameters: The driver for the preparation of products to support routine governance and management will be driven by the frequency of meetings. The anticipated minimum frequency is:
        - Standing (for coordination): VeVA MN Secretariat
        - Once a year: VeVA MN Steering Group (SG).
        - Twice a year (one in person and one virtual): VeVA MN Executive Group (EG), Operational Requirements Working Group and Board (ORWG/ORB), Service Engineering Working Group (SEWG), Service Management Working Group (SMWG), Coalition Interoperability Assurance and Validation Working Group (CIAV WG), CIS Security Working Group (CSWG), Security Accreditation Board (SAB). Note that support requirements for the CIAV WG are covered under SME012.
    - Scope parameters: Routine change management is anticipated to be managed around the monthly meetings of the VeVA MN Change Advisory Board (CAB) and held every month, except when Steadfast Cobalt event is in execution. The scale of each routine change event is anticipated to be no more than:
        - Max Participants: 10 HQs/Units
        - Planning conferences/duration: One 3 day planning conference
        - Test management workshops: One 3 day workshop
        - Services in scope : Up to 10 Services
        - Execution timeline: 1 week
        - Impact assessments of the Requests for Change (RFC) together with support to the change events and V&V will involve staff leading and supporting the ORWG/SEWG/SMWG/CAB/CIAVWG/CSWG with the bulk of effort placed on the SEWG/SMWG/CAB/CIAVWG. Note that support requirements for the CIAV WG are covered under SME012.
    - The service description and costing is valid for the event parameters as described above. Any change in those parameters must be complemented by a relevant Customer Request Form specifying the scope and associated funding, subject to a dedicated project covering requested activities.
- Support VeVA MN Major Change Events. These are events that support a Joining/Exiting Event for units and headquarters supported by the VeVA MN that have defined C2 roles in the DDA FoP.
    - Scope parameters: It is anticipated that these are executed quarterly, except when Steadfast Cobalt event is in execution (i.e. 3x per year). The scale of each major change event is anticipated to be no more than:
        - Max Participants: 15 HQs/Units

        - Planning conferences/duration: One 5 day planning conference
        - Test management workshops: One 5 day workshop
        - Services in scope : Up to 35 Services
        - Execution timeline: 2 weeks
        - Impact assessments of the Requests for Change (RFC) and support to the change events will involve staff that support ORWG/SEWG/SMWG/CAB/CIAVWG/CSWG, with the bulk of effort placed on the SEWG/SMWG/CAB/CIAVWG. Note that support requirements for the CIAV WG are covered under SME012.
    - The service description and costing is valid for the event parameters as described above. Any change in those parameters must be complemented by a relevant Customer Request Form specifying the scope and associated funding, subject to a dedicated project covering requested activities.
- Support the annual Exercise STEADFAST COBALT (STCO). This is an event that supports the annual Ex STCO event that is held to enable the headquarters and units of each new rotation of the Allied Reaction Force (ARF) to join the VeVA MN.
    - Scope parameters: Ex STCO is executed annually, scheduled in the year to enable the ARF to be prepared for its certification exercises. The scale of Ex STCO is anticipated to be no more than:
        - Max Participants: 50 HQs/Units
        - Planning conferences/duration: Four 5 day planning conference with additional meetings for SMA coordination, IER workshop, Academics and Exercise Specification meetings, each no more than 4 days in duration.
        - Test management workshops: three 5 day workshops
        - Services in scope : Up to 35 Services
        - Execution timeline: 3 weeks for PhIIIA (federation Joining V&V), 4 weeks for PhIIIB (federation V&V)
        - Impact assessments of the Requests for Change (RFC) and support to the change events will involve staff that support ORWG/SEWG/SMWG/CAB/CIAVWG/CSWG, with the bulk of effort placed on the SEWG/SMWG/CAB/CIAVWG/CSWG. Note that support requirements for the CIAV WG are covered under SME012.
    - The service description and costing is valid for the event parameters as described above. Any change in those parameters must be complemented by a relevant Customer Request Form specifying the scope and associated funding, subject to a dedicated project covering requested activities.

Service Scope: The following summarizes the expected/anticipated NCI Agency support as described in the ACO directive for the Governance and Management of the VeVA MN.

Support to Routine VeVA MN Governance and Management. NCI Agency staff supporting the working groups and boards of the governance and management structure expected to:

- Support VeVA MN SG and EG Meetings. This can be summarised as:
    - Attendance of meetings by SMA Operating Authority/Design Authority (OA/DA) together with NCI Agency resourced Chairs of WGs and Boards;

  - Attendance of meetings by NCI Agency as the Mission Network Service Provided (MSP) for the NCS provided VeVA Core network (N-VeVA Core, i.e. the Mission Anchor Function (MAF), NATO DCIS and for the static connections between NATO and the Nations).
- Support VeVA MN Secretariat. This can be summarised as:
  - Contribution by WG leads to the maintenance of the Strategic Roadmap (SRM) and the reporting of progress on assigned tasks in the SRM Action Plan;
  - Provision by NCI Agency resourced WG leads of an Annual Report on resourcing issues;
  - Provision by NCI Agency resourced WG leads of support for the preparation and minutes relating to meetings of the EG and SG;
  - Provision by NCI Agency NDW of a series of VeVA MN Governance and Management collaborative workspaces on Internet, NS and upon VeVA MN for access by National MSP, Mission Network Participants (MNP) and prospective HQs and Units needing to join the mission network.
- Support ORWG. This can be summarised as:
  - Contribution by all supporting staff to the maintenance of the SRM and the reporting of progress on assigned tasks in the SRM Action Plan;
  - Contribution by operational analysts to the maintenance of the consolidated Operational Requirements List;
  - Contribution by operational analysts and other supporting staff to the capture and maintenance of the IERs and Information Management Plan;
  - Contribution by all supporting staff to the capture and maintenance of the Gap List.
- Support ORB. This can be summarised as:
  - Attendance of meetings by SMA OA/DA leads together with SME as topic requires.
- Support SEWG. This can be summarised as:
  - Provision of Chair of SEWG;
  - Provision of technical leads for Comm/Core/CoI sub WG;
  - Contribution by all supporting staff to the maintenance of the SRM and the reporting of progress on assigned tasks in the SRM Action Plan;
  - Maintenance of As-Is service topology (architecture) and information to a level of detail to perform RFC impact assessments and service redesign for:
    - Solution Architecture for N-VeVA Core network (esp. federated and xdomain service interfaces);
    - Federation service topology for VeVA Core MN;
    - Confederation service topology for VeVA MN.
  - Support SEWG activities across the Constituent MN (cMN) of the VeVA MN confederation, i.e.:
    - Maintain the Service Strategy;
    - Support SMWG with the maintenance of MN service roadmaps and MN Baselines;
    - Align and maintain JMEI Vol IV;
    - Coordinate definitions of VeVA MN Configuration Item (CI) information attributes;

        - Maintain list of VeVA-wide Authoritative and Trusted Data Sources as identified in the VeVA MN Information Management Plan;
        - Coordinate SEWG of the cMN to perform impact analyses of RFC submitted to the MN Baseline;
        - Coordinate the SEWG of the cMN to perform re-planning of confederation-wide services.
    - Support SEWG activities across the across the MNP of the VeVA Core MN federation, i.e.:
        - Apply extant FMN Spiral Spec to circumstances of the units supported by the VeVA Core MN to support operational requirements;
        - Maintain VeVA Core MN JMEI Vol IV;
        - Support SMWG with maintenance of the Product Baseline, using as a basis the rolling FMN Product baseline;
        - Define federated configuration item attributes of assets critical to the federation of each service;
        - Coordinate provisioning of required COI Service databases through the database deployment plan;
        - Conduct impact analysis of RFC submitted to the CAB;
        - Produce architectural documentation as required to support RFC;
        - Perform the re-planning of services.
    - Provide Planning support and products to:
        - Support SCPG for mission planning;
        - support NPG for mission planning (Resources and tasks are out of scope of SME014);
        - support EPP for those exercises that will use the VeVA (resourcing for attendance at specific MTEP exercise planning conferences out of scope of SME014 as already provided to Business Areas via cSLA);
        - Provide support to
        - Support Operational CIS WG (OCWG) for: SHAPE as SWHQ (via MDSOC ?), ARF, JOA-C, JOA-SE and JOA-NW.
- Support SMWG. This can be summarised as:
    - Provide Chair of SMWG;
    - Contribution by all supporting staff to the maintenance of the SRM and the reporting of progress on assigned tasks in the SRM Action Plan;
    - Support SMWG activities across the cMN of the VeVA MN confederation, i.e.:
        - Align and maintain JMEI Vol I, II and III;
        - Coordinate the pooling of VeVA MN Configuration Item (CI) information attributes;
        - Coordinate the Boundary Protection Services (BPS) to enable the confederation-wide FW management;
        - Provide means to coordinate RFC;
        - Provide means and processes for MN CIS OPCEN coordinate responses to incidents that impact the confederation and provide the means to coordinate events and resolve problems;
        - Provide a forum to align MN Baselines.
    - Support SMWG activities across the across the MNP of the VeVA Core MN federation, i.e.:

        - Align and maintain SMC processes/ Standard Operating Procedures (SOP) for JMEI Vol I, II, III;
        - Maintain the VeVA MN Configuration Baseline;
        - Maintain Forward Schedule of Change;
        - Manage and coordinate the RFCs to the VeVA Core MN Product and Configuration Baselines.
- Support CAB. This can be summarised as:
    - Provide Chair of CAB;
    - Manage the RFC raised by the MNP of the VeVA Core MN and RFC escalated by the CAB of cMN;
    - Coordinate assessments of RFC by ORWG/ORB, SEWG, CSWG/SAB, CIAV;
    - Refer resource-intensive and disruptive changes to EG.
- Provide day-to-day monitoring and management of the VeVA MN. This can be summarised as:
    - Provision of VeVA MN CIS OPCEN. Resources/tasks out of scope of SME014;
    - Provision of VeVA MN Security Operations Centre (SOC). Resources/tasks out of scope of SME014.
- Support CIAV. This can be summarised as:
    - VeVA Governance and Management Support. See Governance and Management package in SME012;
    - Year Round support for VeVA Interoperability Verification and Validation. See Foundation package of SME012.
- Support CSWG. This can be summarised as:
    - Provide Chair of CSWG;
    - Contribution by all supporting staff to the maintenance of the SRM and the reporting of progress on assigned tasks in the SRM Action Plan;
    - Support CSWG activities across the cMN of the VeVA MN confederation, i.e.:
        - Conduct impact analysis of RFC submitted to the CAB;
        - Consolidate and manage the Community Security Requirements Statement (CSRS);
        - Coordinate to ensure common accreditation processes;
        - Coordinate the requirements of security and Cyber Defence policy and supporting directives and guidance that provide for the minimum level of protection and assurance levels are appropriately applied;
        - Coordinate physical and procedural security, CIS Security architecture, CIS Security Accreditation, Information Assurance and PKI coordination, Cyberspace Hygiene, Cyberspace Defence and Cyberspace situational awareness;
        - Maintain the processes for the VeVA MN SOC to coordinate responses to Cyber incidents and to coordinate incident handling with the VeVA MN CIS OPCEN;
        - Provide technical security assessment and recommendations to SAB;
        - Coordinate the preparation of material for the SAB.
    - Additionally support CSWG activities across the across the MNP of the VeVA Core MN federation, i.e.:
        - Maintain a mission focused CSRS;

        - Maintain a mission focused accreditation process.
- Support ORB. This can be summarised as:
    - Attendance of meetings by SMA OA/DA leads together with SME as topic requires.

Support to VeVA MN Major Change Events. NCI Agency staff supporting the working groups and boards of the governance and management structure expected to:

- Support Event Planning. This can be summarised as:
    - Lead SEWG and provide lead SMA DA SME for each service to plan federation of services with MNP. This should include:
        - Production of Planning Products;
        - Tailoring of specific JMEI for event;
        - Provision of assistance to Interoperability Test Director (IOTD) in transferring planning products into IO Core.
    - Provide IOTD team to lead CIAV WG - see SME012;
    - Lead SMWG and provide SMA OA SME to align SMC processes of MNP;
    - Provide CAB Chair and fulfil SMA roles in CAB called for event;
    - Lead CSWG and provide CS SME expertise;
    - Attend any SAB called for event (SMA OA/DA and CS SME).
- Support event execution and reporting. This can be summarised as:
    - Provide technical oversight (SMA DA service leads).
    - Provide change manager and configuration manager.
    - Provide IOTD, test environment, test directors and execute test plan - See SME012
    - Contribute to interoperability and evaluation reports

Support to annual Exercise STEADFAST COBALT (STCO). NCI Agency staff supporting the working groups and boards of the governance and management structure expected to:

- Support Exercise Scoping. This can be summarised as:
    - Provide SMA and IOTD input to EXSPEC
- Support Exercise planning conferences. This can be summarised as:
    - Lead SEWG and provide lead SMA DA SME for each service to plan federation of services with MNP. This should include:
        - Production of Planning Products;
        - Tailoring of specific JMEI for exercise;
        - Provision of assistance to IOTD in transferring planning products into IO Core.
    - Provide IOTD team to lead CIAV WG - see SME012;
    - Lead SMWG and provide SMA OA SME to align SMC processes of MNP;
    - Provide CAB Chair and fulfil SMA roles in CAB called for exercise;
    - Lead CSWG and provide CS SME expertise;
    - Attend any SAB called for exercise (SMA OA/DA and CS SME).
- Support exercise execution and reporting
    - Provide SMA DA service lead technical oversight
    - Provide change manager and configuration manager.

  - Provide IOTD, test environment, test directors and execute test plan - See SME012
  - Contribute to interoperability and evaluation reports

Travel. Due to the meeting and exercise schedule of Exercise STCO and the need to travel to planning conferences of the major change events, there are Travel costs associated with this service.

Service Request: The service can only be requested as follows:

- ACO funded: via the CSLA (SLIN10);

Service Flavours: The Service is available in various flavours:

Fixed packaging delivering:

- Support to Routine VeVA MN Governance and Management.
- Support to VeVA MN Major Change Events
- Support to annual Exercise STEADFAST COBALT (STCO)

Available on: The SME can provide services/advice through the following networks:

- NATO SECRET
- NATO SECRET Releasable to VeVA.

Service prerequisites: N/A

Standard Service Support Levels*:* N/A

Available/Related NCI Academy Training not covered by service cost:

A0104	NATO CIS Planning

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery. The service charge should take into account the TDY commitment.

SME017 NATO Collaboration Solutions Expertise Service

Service ID: SME017

Service Name: NATO Collaboration Solutions Expertise Service

Portfolio Group: Subject Matter Expertise Services

Service Description: This Service provides advice, guidance, business analysis, design and implementation support for new and existing Collaboration Solutions. The Service transforms customer requirements into tangible solutions that are in-line with most current Alliance's policies and directives. The Service facilitates the fulfilment of the need for collaboration within NATO enterprise, as well as between NATO and its external partners.

Value Proposition: The Service ensures that Collaboration Solutions are tailored to unique information-related needs of a customer while being in line with NATO Enterprise policies and guidance on Information and Knowledge Management (IKM), Information Security, Communications, Visual design and more. The added value is measured in terms of better compliance with standards, more effective collaboration with version control, sharing and distribution and overall fit for purpose capability.

Service Features: The Service provides the following features:

- **Collaboration Services Business Analysis**: Provide SME expertise on reaching collaboration goals and objectives using technical capabilities within the boundaries established by NATO polices on Web Applications, Information Security and Information and Knowledge Management.
- **"Proof of Concepts" and Prototypes**: Create "proof of concepts" or prototypes, focused on improving collaboration tools and end-user experience within NATO enterprise and its institutional and national partners based on the customer's requirements.
- **Collaboration Solutions design:** Advice on design, content architecture and visual identity that responds to collaboration goals and target audience expectations. That includes advice and guidance on creation and maintenance of user access groups' architecture and mapping.
- **Collaboration Features design**: Advice on the most suitable choice and configuration of the collaboration tools. Design and architecture of workflows that focus on enriching digital collaboration environment within and between groups of users i.e. document collaboration, approval, registration and more.
- **Alignment with NATO Enterprise regulations**: Assure that collaboration services are built in accordance to NATO rules and regulations, and best practice such as Information and Knowledge Management, information and web applications security, NATO Visual Identity guidance, etc.
- **Collaboration Services Quality Assurance**: In close collaboration with project team and customer, the role leads quality assurance efforts to make sure the final product meets functional expectations and requirements.
- **Collaboration Services Analytics**: Collect and analyse data in order to suggest tangible solutions for improvements of Collaboration Services.
- **Identity and Access Privileges Architecture and Management:** Advice and guidance on creation of permissions groups' architecture and mapping. Practical

advice on good practices related to daily maintenance and management of user groups and their permissions. Identity and Access Privileges management.

- **Metadata Management configuration**: Alignment with NATO Core Metadata Specification (NCMS), configuration and creation of metadata and associated NATO Document Types: Memo, Letter, Technical Note (TN), RFQs and alike.
- **Portal Configuration**: Apply and configure out of the box web applications and features such as: Libraries, Lists, Views, Workflows, Wikis, Blogs, and other SharePoint elements. Configuration of existing portals towards being compliant with requirements for NATO Standard Portals.
- **Web Content Authoring and Management**: Content creation and upload.
- **Documentation**: Production of designs, policies, directives, training guides, user guides and dedicated analysis in the collaboration portal arena.
- **Data migration**: Plan and execute data migration between NATO information management systems.
- **Training design and delivery**: Assess and advise on customer need for training, align its scope, delivery method, and schedule accordingly. On-site and on-line delivery of trainings to end users and to functional administrators. Produce training materials (i.e. manuals and instructions).

Service Flavours: The service is available as a single flavour.

Available on:

Internet
NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

Service prerequisites: None.

Standard Service Support Levels: N/A.

Service Cost / Price: The Service is priced “per hour” (A3 equivalent), in accordance with the valid NCI Agency Customer Rates.

SME021 C2 Data Integration and Management Service

Service ID: SME021

Service Name: C2 Data Integration and Management Service

Portfolio Group: Subject Matter Expertise Services

Service Description: The C2 Data Integration and Management Service provides Subject Matter Expertise (SME) on efficient C2 system integration between NATO and national Function Area Systems (FAS) for interoperability, automation, data exploitation, fusion and modelling. This service leverages existing various methodologies and tools, including NATO, national and industry FAS in order to provide optimal engineering solutions. Solution identification shall consider cost, technical complexity, robustness and maintainability.

Value Proposition:

This C2 data integration service will provide the following benefits to the customer:

- Support the transition of the user environment from a system-centric towards a data-centric battlespace
- Provide comprehensive and streamlined solution engineering for system and data integration including:
    - Translation of user requirements into efficient C2 data integration solutions
    - Optimization of operations through integration of disparate data sources
    - Bridging of dissimilar systems by establishing interoperability solution in local national or mission environment
    - Translation, fuse, analytics and augmentation of data for consumers in a required format, protocol and information product
    - Analytics and reporting: providing valuable insights into data trends and patterns, enabling organizations to make informed decisions based on accurate and up-to-date information.
- Team of experts with cutting-edge technology and best practices knowledge
- Improves decision-making and operational efficiency
- Improves situational awareness throughout the battlespace
- Enhances interoperability within NATO and nations between FAS

Service Features: The C2 data integration and management service features the SME for C2 FAS integration for data exploitation, analytics, modeling and dissemination. Focusing on streamlining data integration and management processes, supporting organizations save time and resources, enabling focus on core business operations.

The service shall provide a problem analysis and identification of solution options with associated benefits, shortcomings and costs.

Service Flavours: This service is tailored to meet individual needs of a customer, based on the complexity and scope of the data integration and management problem to be solved.

- Remote support – Available
- On-site support – Available
- Complete Solution – Available may include remote and on-site support as required

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret
Availability on any other security domain is TBC for a New Service Request.

Service Prerequisites:

Subject to license agreement and MOUs

Standard Service Support Levels:

Service Availability Target: n/a

Service Restoration: n/a

Service Cost/Price[1]: Cost model is be based on level of effort. The unit of measure for the Service is Per Defined Service. Cost for each defined service is individually set up, in accordance with agreed scope and conditions of the service delivery, as well as valid NCI Agency Customer Rates.

Cost calculations are based on NCI Agency rates.

SME022 Maritime Broadcast Operations Service

Service ID: SME022

Service Name: Maritime Broadcast Operations Service

Service Type: Customer Facing

Portfolio Group: Subject Matter Expertise Service

Service Status: "*Available" for 2024 if approved*

Service Description: This service provides the 24/7 ability for MARCOM to manage the delivery of formal military messages onto selected HF and VLF maritime broadcasts.

Value Proposition: MARCOM is the Broadcast Control Authority for multiple High Frequency and Very Low Frequency broadcasts, used to maintain Command and Control of Nations' vessels when placed under MARCOM C2. This service enables designated vessels to be included within specified MARCOM broadcasts, the inclusion of formal messaging traffic onto those broadcasts and the assurance of the effectiveness of the broadcasts.

Service Features: The Maritime Broadcast Operations Service includes the following broadcasts:

HF. Extends the formal messaging service onto specified NATO High Frequency (HF) broadcasts for units designated by MARCOM, as the "Broadcast Control Authority":

1. Coordinate the inclusion of units designated by MARCOM onto the NATO X11C broadcast, including Routing Indicators and Guard List.

2. Handle traffic exceptions for traffic being directed to X11C broadcast.

3. Manage Over The Air Distribution (OTAD) for X11C broadcast.

4. Provide cover for the X11B broadcast managed by UK Commcen Plymouth, as part of and as directed by higher level NATO HF broadcast coordination.

VLF. Extends the formal messaging service onto the NATO Very Low Frequency (VLF) broadcasts for units designated by MARCOM SUBSUBNATO, as the "Submarine Operating Authority":

1. Coordinate the inclusion of units designated by MARCOM onto the NATO VLF broadcast, including Route Changes and Guard Lists.

2. Manage the inclusion of messages when directed by MARCOM onto MARCOM broadcasts.

3. Conduct Over The Air Monitoring (OTAM) of MARCOM broadcasts to assure MARCOM that the broadcast is functional.

4. Monitoring the VLF network of VLF transmitters, receivers and others nodes, advising MARCOM of any service impacts and mitigations.

Service Request: This service is coordinated with and operationally directed by MARCOM.

Service Flavours: This service is available as a single flavour.

Available on: NS

Service Prerequisites: The service relies upon APP029 Military Messaging Application Service, INF013 VLF Broadcast Service (that provides the VLF interconnection network), CSU Northwood local service support to MARCOM for support to the 2 CMX servers (primary and backup) and 3 workstations, and upon agreements between ACO and the UK for the provision of UK HF and VLF transmitters and receivers.

Standard Service Support Levels*:* Any incidents impacting the service need to be submitted through the NCIA ESOC. The service consists of military personnel within CSU Northwood, plus the CMX software that is supported under annual contract with Raytheon Systems Limited, UK.

Service Availability[1] Target: 95%

Service Restoration: There are no formal service restoration targets for this service. The Raytheon support contract provides 8-hour response during normal working hours (Mon-Fri 0900-1700).

Service Cost / Price:

The service is a non-unitised service. The service cost is the approved NCIA overhead cost for the specific level of Commcen Northwood effort assigned to the operation of the maritime broadcasts, 10.75FTE military personnel, plus the annual cost of the CMX software support, enabled through UK MOD DE&S contract number GCS/00002 Amendment 1 dated 30th January 2008.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100

**Minutes available during agreed reporting period excluding planned maintenance minutes*

This page is left blank intentionally

Application Services

This page is left blank intentionally

APP001 Approved Commercial-off-the-shelf Products Procurement Service

Please note that this service offering is for the provisioning of Commercial-off-the-shelf (COTS) software licenses and software support renewals. The products requested must be in the pool of the NCI Agency Approved Fielded Products List* (AFPL).

The costs for these products under this service are solely for the license procurement and/or annual software support renewal costs of the software license requested. It does not include any manpower support to package/install/maintain the application.

*If the product is not in AFPL, customers can choose to submit a separate CRF (Customer Request Form) in order to request the addition of this application to AFPL. The Agency applies a series of AFPL testing procedures before it can confirm that the application can be added to AFPL or not, thus separate costs apply to such requests and are not considered within the scope of APP001.

APP002 Shared Early Warning (SEW) Application Service

Service ID: APP002

Service Name: Shared Early Warning (SEW) Application Service

Portfolio Group: Application Services

Service Description: The Shared Early Warning (SEW) Application Service provides the user with NATO's 24/7 early warning capability to disseminate Tactical Ballistic Missile (TBM), provided by US national capabilities, to NCS HQs, NATO HQ and political representatives in NATO nations.

Value Proposition: The SEW Application Service provides standardised NATO warning and situational awareness of ballistic missile threat launches to support situation awareness, high-level political and military consultation and decision making.

Service Features: The SEW Application Service provides visual and audio alerts when each ballistic missile launch is reported. Also, the SEW application service visualizes the reported launch and predicted impact points on map displays. Past missile launches can be reviewed, including key data on threat characteristics.

Service Flavours: The service is available as 2 flavours:

APP002 Centralised Capability

APP002F Federated Service: This service flavour provides federation support to NFS and Nations for authorization, configuration and troubleshooting of their connections to an SEW Service Delivery Point (identified as centralized NCS CoI servers).

This flavour also encompasses Application changes triggered by federation requests and compensation for capacity increase required by the increasing demand on corresponding centralized infrastructure.
This service flavour ensures initialization and continuity of the COI interconnections between Nations & NFS with NCS. Troubleshooting beyond NATO Interconnection Point on the national or NFS side is not included in this service flavour. The service flavour includes:

- Management of technical connectivity to centralized NCS COI servers given the requester has authorization from SHAPE and the corresponding NCS party
- Troubleshooting on configuration of the connection to centralized NCS COI servers
- Application service delivery monitoring & corrective actions
- Application changes triggered by this federation request
- Compensation for capacity increase as per the increasing demand on corresponding NCS CoI servers

SME007 service is recommended to complement this service flavour, would the Customer have connectivity in B2B mode. This is recommended for support beyond NIP.

Available on:

NATO Secret

Service Prerequisites:

WPS001 Managed Device Service

For APP002F flavour: Network connectivity for NIP interconnection with NATO centralized network (NS)

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Centralised flavour of the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

For the Federated flavour the unit of measure for the Service is per connection.

APP005 CBRN Application Service

Service ID: APP005

Service Name: CBRN Application Service

Portfolio Group: Application Services

Service Description: The Chemical, Biological, Radiological, and Nuclear (CBRN) Application Service provides functions that enable CBRN Community of Interest to support the three pillars of CBRN Defence – Prevent, Protect and Recover.

Value proposition: The service is integral to the NATO CBRN Community of Interest and offers the following benefits:

- Development, acquisition, and maintenance of CBRN software applications in accordance with the NATO specific requirements and the latest doctrine.
- Provision of state of the art service assets that support the CBRN community to:
    - maintain CBRN situational awareness in operations;
    - calculate the NATO approved Hazard Areas and Contaminated Areas for all types of CBRN incidents;
    - risk assessment and what-if analysis of known or potential hazards within operational areas;
    - generation of exercise planning material based on pre-planned incidents;
- Training and mentoring in the usage of CBRN applications assets in support of NATO missions.

Service Features:

- Centralised acquisition and management of CBRN software licenses;
- Support of the software accreditation process for NATO security domains;
- Installation and configuration of software application instances;
- Operational Support
    - Centralised routine support: **t**he regular maintenance of the software applications in the NATO networks requires a set of routine maintenance activities:
        - Overall service management and planning;
        - Communication of the service roadmap;
        - Support and maintain the accreditation of the CBRN application assets;
        - Centralised support provided to the CBRN community of interest;
        - Analysis of incidents and problems related to the operation of CBRN applications;
        - Coordination of the investigation of issues and requirements with the respective software vendors;
    - Specific service instance support: provides the required individual support services to the specific sites at charge and may include:
        - Support to design, planning and implementation of the CBRN Application Services on the end user devices;
        - Acquisition of the respective software licenses and export authorisations;

    - Provision of a training session for the user community;
    - Online support regarding incidents related to the installed application assets;
    - Implementation of the required software updates on the end user devices in accordance with the service roadmap.
- Training and Mentoring on the usage of CBRN applications aligned with the NATO doctrine and best practices.

The Service includes the following software-application assets:

- **CBRN Analysis**:

  An advanced, COTS-based CBRN information management application that includes Hazard Prediction and Warning and Reporting (W&R). Provides users with rapid and accurate information to increase their CBRN situational awareness within an area where CBRN materials may be used. CBRN-Analysis effectively supports and enhances risk-management in all phases of an operation, both in the planning and pre-deployment phase, in-theatre and in the post conflict or recovery phase.

- **Hazard Prediction and Assessment Capability (HPAC):**

  HPAC models the release of Chemical Biological Radiological and Nuclear (CBRN) materials to the atmosphere and the associated dispersion using detailed meteorological information.
  Note: SHAPE governs the release of this application.

Service Flavours: The Service may be fully customized to meet requirements of a specific customer or a specific site.

Available on:

NATO Unclassified
NATO Secret
Mission Secret

Service prerequisites:

WPS001 - Managed Device Services (for application instances installed on NCI Agency managed networks)

Standard Service support levels:

Service Availability Target: 95.0%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident is 4 hours. Availability of the “CBRN application service” is primarily dictated by the availability of the underlying Managed Devices Service.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP006 Ballistic Missile Defence (BMD) System of Systems Management Service

Service ID: APP006

Service Name: Ballistic Missile Defence (BMD) System of Systems Management

Portfolio Group: Application Services

Service Description: The APP006 service provides coordination and orchestration of In Service Support activities related to BMD System of Systems including interoperability assurance, integration and lifecycle management, and provides the Shared Early Warning Plus service (SEW+I). The service also provides the primary interface between the customers and users (Operational BMD Community) and all NCI Agency Units devoted to perform In-Service Support (ISS) for the BMD Command Control Communication and Information (BMDC3I) System of Systems. The service does not take over or duplicate any of the below defined BMDC3I services.

The BMD capability: Provides full coverage and protection for all NATO European populations, territory and forces against the increasing threats posed by ballistic missiles. This also includes required protection of deployed forces and high value assets/areas within an area of operations/interest from attacks by ballistic missiles. BMD interlinks all levels of military command from the military strategic level down to the tactical level, all across NATO, regardless of the country or the respective military service. BMD is a combined and joint capability.

BMD System of Systems: The NCI Agency IT Systems (products and services), in support of the BMD capability, provide functions that enable NATO Commands to integrate sensor information, build and distribute a comprehensive and real-time BMD operational picture, and exercise command and control of voluntary national contributions (sensors and effectors) provided by Allies. The application Air Command and Control System TMD1 (APP050) is the core integrator of the BMD functions.

The BMDC3I systems are in use at the Ballistic Missile Defence Operations Centre (BMDOC) in Ramstein and multiple other NATO Command Structure sites. The following products and services enable the BMD capability and compose the BMDC3I System of Systems:

Customer facing services:

- APP002 (SEW Application Service) Shared Early Warning
- APP007 (TOPFAS Application Service) - Tool for Operations Planning Functional Services
- APP015 (JCHAT Application Service) - Secure Tactical Joint Chat
- APP022 (NCOP Application Service) - NATO Common Operational Picture
- APP049 (ICC Application Service) - Integrated Command and Control (includes LSID)
- APP050 (Air Command and Control System TMD1)
- APP061 (AirC2IS Application Service) - Air Command and Control Information System

- WPS014 (Secure Voice Service)
- WPS015 (Voice Loop Service)

Underlying services:

- APP010 (NIRIS Application Service) - Networked Interoperable Real-Time Information Service
- APP011 (OANT Application Service) - Online Analyser for Networked Tactical-Data
- APP012 (SMACQ Application Service) - Service to Monitor and Assess Connectivity and Quality
- PLT013 (NISP Service) NATO - Integrated Secure Platform
- APP055 (Core Geographic Information System -GIS- Application Service)
- WPS002 (Enterprise Identity Access Management Service)
- WPS003 (Enterprise User License Service)
- PLT001 (Information Sharing and Collaboration Platform Services)
- WPS012 (E-mail Service)
- PLT003 (Web Hosting Service)
- SEC011 (Gateway Security Service)
- INF001 (LAN Service)
- INF002 (NATO General Purpose Communication System (NGCS) Point of Presence (PoP) Service)
- INF004 (Infrastructure Virtualization Service)
- INF005 (Infrastructure Integration Service)
- INF006 (NATO Enterprise Directory Service -NEDS)
- INF007 (Infrastructure Storage Service)
- INF014 (Transmission Service)
- INF018 (Deployable CIS Mini-Point of Presence (PoP)
- INF040 (UHF TACSAT Radio Services) - Tactical Satellite

The actual BMDC3I service composition for operational use depends on the customer's operational requirements. NCI Agency configures the required composition in close cooperation with the customer.

All above listed BMDC3I services operate on the NATO General Communications System (NGCS) network at Wide Area Network level. Nations provide feeds through NATO-National static gateways or through NATO deployable CIS equipment.

Value proposition: The Service main objective and value is to maintain the availability, integrity and alignment of the fielded BMD Command Control Communication and Information (BMDC3I) System of Systems and the IT services provided by NCI Agency for BMDC3I. The service also provides coordination of actions for BMD In-Service Support related aspects and issues for NATO BMDC3I customers and users.

Service Features: The APP006 service manages the following in support of BMDC3I system of systems:

- the BMD SoS Delivery Plan in accordance with the BMD SoS Service Tree.

- The supervision of the processing of ISS ITSM BMD related Tickets (Incident, Services Requests) through their lifecycle and monitoring iaw SLA levels.
- the processing of ISS BMD related L-ECPs, and monitoring of their implementation plan/execution.

  the relationship with CSU Ramstein and BMDOC users: Ensure day-to-day coordination with them related to BMD Standing Mission, NS2T Mission, technical evaluation activities, Site Support Manager Role and CAB chairmanship.

- BMD Obsolescence Management: Manage BMD SoS obsolescence; maintaining risk review and gap analysis of the SoS and interconnecting systems in coordination with other Service Lines and system owners. This analysis will consider programmatic and funding mechanisms to ensure the SoS components and services are supported throughout the lifecycle.

Service Flavours: The service is available as a single flavour

Available on: N/A

Service prerequisites: None

Standard Service Support Levels: N/A. The APP006 service supports at coordination level all NCIA Service Lines to provide In-Service Support in accordance with requirements as agreed between the Customer and NCI Agency for BMDC3I related services).

Available NCI Academy Training not covered by service cost:

A1027	APP006	BMD Planning with AirC2IS

Service Cost / Price: The unit of measure for the Service is 1. NCI Agency charges the total of the Service delivery in accordance with specifically arranged conditions of the Service delivery. The service APP006 does not duplicate any of the service delivery costs for the above-mentioned BMDC3I System of Systems services.

APP007 TOPFAS Application Service

Service ID: APP007

Service Name: Tools for Operations Planning Functional Services (TOPFAS) Application Service

Portfolio Group: Application Services

Service Description: TOPFAS (Tools for Operations Planning Functional Services) Application Service provides the user with integrated collaboration planning and decision support capabilities. This service is comprised of multiple modules that support Systems Analysis, Operational Planning, Order of Battle (ORBAT) management and Assessment of Operational Campaigns. This service also offers complete support for the NATO Force Generation Management process and Readiness Reporting as well as non-Intel Request For Information (RFI) Management.

Value proposition: TOPFAS Application Service offers the user (through the suite of available modules) a distributed, multi-level and a collaborative environment that benefits standardization, productivity and quality to operational planning processes.

TOPFAS offers a unique combination of desktop applications, web applications and portal to provide dedicated tools and information dissemination to each community of interest.

Furthermore, the TOPFAS Application Service also contributes to the Ballistic Missile Defence capability through integration of specific functions and interfaces for BMD, in particular with AirC2IS.

Service Features: The TOPFAS Application Service is comprised of the following applications:

- TOPFAS Systems Analysis Tool (SAT) – Supports systems analysis of the engagement space for holistic situational awareness and understanding.
- TOPFAS Operations Planning Tool (OPT) – Campaign planning tool that supports the development and synchronization of strategic options, operational and tactical courses of action
- TOPFAS Campaign Assessment Tool (CAT) – Supports measuring progress towards the planned campaign end-state.
- TOPFAS ORBAT Management Tool (OMT) – Supports building and viewing order of battle (ORBAT) information and allows for management of national and NATO Response Force (NNRF) ORBATs.
- TOPFAS Web Portal and Applications (TWP) – Provides TOPFAS information content to be shared with wider communities of interest through an internet portal as well as dedicated applications for Wiki, RFI, Videos, etc.
- TOPFAS NATO Crisis Response System (NCRS) Applications – Web based tool – Supports the formal declaration and approval processes of Crises Responses Measures by SHAPE and Nations.
- TOPFAS enhanced Force Generation Management Tool (eFGMT) – Web based tool – Supports the complete NATO Force Generation cycle with nations

- TOPFAS Readiness Reporting Tool (RRT) – Web based tool – Supports the evaluation readiness of the NATO Response Forces or coalition forces
- TOPFAS Operational Capability Concept (OCC) Evaluation and Feedback (E&F) Tool – Supports partner efforts to develop forces that are fully interoperable and capable of operating with NATO

In addition, these services include the delivery and maintenance of support applications and portals:

- TOPFAS User Management Tool (UMT) – Allows TOPFAS functional managers to manage user access and roles
- TOPFAS Data Management Tool (DMT) – Allows TOPFAS reference data and configuration management
- TOPFAS Support Portal – Information SharePoint portal;
- TOPFAS Help Centre - Online help, Computer Based Training and support portal.

Service Flavours: TOPFAS Application Service can be fully customised and provided with different components enabled/disabled. Some applications (e.g. OCC) can be used independently.

Available on:

NATO Secret, Mission Secret

If you require availability of any other security domain please raise this as a New Service Request.

Service prerequisites:

WPS001 – Managed Device Service

APP055 - Core GIS Geospatial Services

Standard Service support levels:

Service Availability Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A0264	TOPFAS System Administrator
A0265	TOPFAS OPT for User
A0266	TOPFAS SAT for User
A0267	TOPFAS CAT for User
A0285	TOPFAS OPT Train the Trainer
A0286	TOPFAS SAT Train the Trainer
A0287	TOPFAS CAT Train the Trainer
A0288	TOPFAS for Advanced User-Functional Manager

A9067	eFGMT Functional Manager
A9068	eFGMT Practitioner

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP009 Integration CORE (INT-CORE) Application Service

Service ID: APP009

Service Name: Integration CORE (INT-CORE) Application Service

Portfolio Group: Application Services

Service Description: The Service provides Integration Core (INT-CORE) specialist data management toolbox as a mission configurable capability allowing for rapid adoption of new data sources and on-demand configuration of heterogeneous systems, to support information exchange capabilities between entities on the network, even when entities have dissimilar systems.

Value Proposition: At the highest level, the functionality to be provided through the INT-CORE Application Service is to ingest data from a variety of data sources and to transform that information into forms that can be consumed by other systems in the network. To achieve a higher level of integration and interoperability, INT-CORE enables data sources to provide information to consumer systems and/or authorized individuals and enables consumers to discover, subscribe to or request information. INT-CORE is designed and developed with an approach that will provide a flexible foundation to significantly improve interoperability.

Service Features: The INT-CORE Application Service features the ability for ingestion, dissemination and transformation of data in an interoperable manner based on NATO and commercial standards.

- Mission-configurable data management toolbox to bridge emerging information exchange problems,
- Improved information exchange across communities of interest,Provision of information to consumers in a protocol they use (e-mail, XMPP, web services, portal, etc.),
- Provision of information to consumers in a format they use (NVG, KML, Plain Text, Native, etc.),
- Provision of information to consumers in a required data model
- Enabling easy configuration of the system for different kinds of data for rapidly changing mission environment at runtime,
- Improving access to Battle Space Objects, providing data augmentation
- Provision of content to the support building of unified mission Common Operational Picture (COP),
- Optimizing bandwidth through a filtering, by moving towards a geospatial push/event based architecture,

Provision of system administration, monitoring, error handling and error notification capabilities

The main supported interfaces for data collection and exchange are:

Interface categories	Standard / Protocol	Version	Direction
Data services	NVG	1.4/1.5/2.0	In + out
	Open Search	-	In + out
	KML	1.0/2.2	In + out
	ODBC	-	In
	TAK CoT	-	In
	IMAP / POP3 / EWS	-	In + Out
	SharePoint	2007-2021	In + out
	Generic XML messages	-	In + out
	JSON/GeoJSON	-	In + out
	Publish/Subscribe (WS-Notification)	-	In + out
	AdatP-3	Any	In + out
	MOSS	MOSS 2007 - 2021	In + Out
	XMPP	-	In + out
	HTTP	-	In + out
	TCP-IP	-	In
	REST	-	In +out
	RSS	-	In + out
Functional systems services	AirC2IS	-	In + out
	ANET	-	In + out
	CIDNE	2.8.4+	In + out
	TAK	-	In

	CSD	3.4+ / 3.8.1	In
	Sitaware	-	In + out
	iGeoSIT	-	In + out
	JOCWatch	-	In
	JTS	-	Out
	LC2IS	-	In + out
	LOGFAS	-	In + out
	MIDB	-	In
	IntelFS	-	In + out
	NCOP	-	In + out
	CBRN	-	In + out
	SEW	-	In +out
	JChat	-	In +out
	NATO MEDICS	-	In

Table 1: INT-CORE available interfaces overview

Service Flavours:

- APP009-1 Large Site
- APP009-2 Medium Site
- APP009-3 Small Site

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

Note: Instances will be provided on the different security domain based on New Service Request.

Service Prerequisites:

INF004 Infrastructure Virtualization Service

Standard Service Support Levels:

Service Availability Target: 98% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

Service Cost/Price: The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP010 NIRIS Application Service

Service ID: APP010

Service Name: NIRIS Application Service

Portfolio Group: Application Services

Service Description: The NIRIS (Networked Interoperable Real-Time Information Service) Application Service provides situational information in support of automated (Air) C2 and information systems as well as BMD System of Systems within NATO. The NIRIS Application Service does this through the enablement of data collection, dissemination and transformation to information in an interoperable manner, based upon NATO and Commercial standards.

Value proposition: The NIRIS Application Service is integral for communities of interest within Air, Land, Maritime, Joint, Logistic and Intelligence domains. The NIRIS Application Service acts as a middle layer between data producers and information consumers (e.g. ICC, AirC2IS, iGeoSIT and NCOP) making information collected from multiple sources available to decision makers (as services) as Battle Space Objects (BSO). The key values of NIRIS are:

- Provision of (near) real-time situational awareness for operations.
- Wide range of supported interfaces for data collection and exchange strongly supporting interoperability.
- Harmonised view via BSO's on the collected data with access to in-depth detail to support decision makers.
- Allows integration via several standardised interfaces with other NATO and National systems.

Service Features: The NIRIS Application Service features the ability for data collection, dissemination and transformation of data in an interoperable manner based on NATO and commercial standards. Furthermore, it provides services to perform data format conversions, recording/replay and track augmentation. Management of NIRIS is offered by a modern, web-based user interface offering full, role-based access to the various capabilities. A key feature is the versatility of its interoperability while maintaining focus on standard's compliance.. The main supported interfaces for data collection and exchange are:

- Link1 (STANAG 5501) – Air Picture
- Link 11B (STANAG 5511) – Maritime, Air Picture
- Link 16 (STANAG 5516) – Air, Ground, Maritime, BMD Picture
- JREAP (STANAG 5518) – Transport for Link 16
- VMF (STANAG 5519) – Ground Picture
- Link 22 (STANAG 5522) – Maritime, Air Picture
- OTH-Gold – Maritime, Ground, Air Picture
- NFFI ("D" Doc) – Friendly Force Tracking (Ground) Picture
- FFI-MTF-XML (STANAG 5527) – Friendly Force Tracking (Ground) Picture
- SIMPLE (STANAG 5602) – Transport for Link 11, Link 16, Link 22, DIS (for IO testing)
- ITV and VATS – Civilian Convoys
- Automatic Identification System (AIS) – Civilian Maritime Picture
- Eurocontrol ASTERIX (including ADSB) – Civilian Air Picture and Air Traffic Control

The collection and exchange is utilizing standard protocols where available (both IP and serial). The NIRIS Application Service offers full hub capabilities for e.g. Link16/JREAP, SIMPLE and FFT, including extensive filtering options.

The main supported interfaces for data and information consumers are:

- Trackstore integration (via API) – Provision of (near) real-time BSO information
- NVG (NATO Vector Graphics) – BSO overlays via web-services
- RESTful Track Service (JSON) – Provision of near real-time BSO information
- KML (Keyhole Mark-up Language) – BSO overlays via web-services
- SIP3 – Friendly Force Tracking information via web-service interface (NFFI, FFI)
- WSMP (Web Service Messaging Protocol)

Service Flavours: The service is available as a single flavour.

Available on:

NATO Unclassified
NATO Secret
Mission Secret
Availability on any other security domain is TBC upon a New Service Request.

Service Dependencies:

SEC011: Security Certificate Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A1012	NIRIS SYSTEM ADMINISTRATOR
A1028	NIRIS SYSTEM ADMINISTRATOR UPDATE (NIR-UP)

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP011 OANT Application Service

Service ID: APP011

Service Name: OANT Application Service

Portfolio Group: Application Services

Service Description: The OANT (Online Analyser for Networked Tactical-Data) Application Service provides the user with a quick and easy way to analyse C4ISR data flowing on operational, test and/or exercise networks. OANT Application Service provides compliancy reports to agreed NATO Standards, plus providing Revision, Extract and Report capabilities on the logical connectivity of the data flows. Furthermore the provision of capability in the checking of data quality.

The OANT Application Service provides a both a thick client (OANT SWING) and a web-based net-enabled service (OANT WEB) interface for data monitoring, analysis and reporting, supporting various operational data exchange formats and protocols, such as: JREAP, GMTI, Link 16, Link 11, Link 1, NFFI, FFI, DIS and OTH-G.

Value proposition: The OANT Application Service provides its users with the following number of key benefits:

- NATO Standardization and Standards V&V bodies: test and verify quality and improve content of STANAGs for completeness, correctness, ambiguities and vagueness.
- War fighters (J3 and J6): up-to-date web access to shared assessments and improved situational awareness of data flows, connectivity and exchanged data quality, increasing trust in the information used to support decision making.
- OPS and interoperability event network, service management and control and analysis groups: smarter, improved and shared means of monitoring connectivity and data quality, to identify, understand and troubleshoot data and interoperability issues in a timely manner.
- System/Service developers: cost and time-savings with improved insight into STANAG compliancy and data content of exchanged messages to support self-analysis and continuous “pretesting” in order to foster out-of-the-box plug-and-play interoperability.

Service Features: The OANT Application service is comprised of the following features:

- Enablement of one-to-one mapping between Standard Specifications and the way OANT interprets messages, words and fields
- Interpretation of received messages from bits and bytes into human readable information
- Assessments of received message contents against applicable standards leveraging on XML generated metadata and data specifications captured in-line with the STANAG/Standards Transformation Framework (STF) Design Rules (NISP, 2014)

- Collection and reporting of statistics on received data (including but not limited to breakdown per payload format, message originator, message label and encountered error type)
- Provision of further insight in to derived message information (e.g. track information)
- Interface for data monitoring, analysis and reporting, supporting various operational data exchange formats and protocols, such as JREAP, GMTI, Link 16, Link 11, Link 1, Link 22, VMF, SIMPLE, NFFI, FFI, DIS and OTH-G.

In addition, the OANT-WEB service flavour offers the following features: provision of analysis and verification of a data forwarding process; comparing both the input the stream and the forwarded data stream; and providing an assessment of whether the forwarding occurred in accordance with the applicable data forwarding standard.

Service Flavours:

OANT SWING – a thick client application run on a workstation
OANT WEB – designed to be deployed in a distributed environment

OANT Web flavour is required in order to be able to provide data to the SMACQ Application Service for further analysis of data connectivity, timeliness and quality, to provide an aggregated and historical view on these measurements collected from various sources.

SMACQ and OANT together form the C2 IOTA (C2 data Interoperability & Traffic Assessment) Services Suite.

Available on:

NATO Unclassified
NATO Secret
Mission Secret
The Service may be available on other networks upon a New Service Request.

Service Prerequisites:

WPS001 Managed Device Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A1012	NIRIS SYSTEM ADMINISTRATOR

Service Cost/ Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP012 SMACQ Application Service

Service ID: APP012

Service Name: SMACQ Application Service

Portfolio Group: Application Services

Service Description: The SMACQ (Service to Monitor and Assess Connectivity and Quality) Application Service provides the user with capability to monitor data exchange of operational information dissemination networks to assess and report on its logical connectivity and quality based on Standards. SMACQ leverages and combines information obtained from OANT (APP011) and/or NIRIS (APP010 Application Services, to provide further analysis of data quality KPIs, such as connectivity, timeliness, activity and compliancy, insights on historical trends and changes of these KPIs via statistical reports and an overall aggregated graphical view via simple traffic colour-coded indicators.

Value Proposition: SMACQ Application Service offers the following key benefits for a wide range of users including but not limited to following:

- Commanders, as SMACQ is monitoring and reporting on the full data flow quality, it provides Decision-makers with an enhanced situational awareness and higher increase in the trust on the data they are using to make more effective decisions.
- War fighters (J3 and J6), usually having an isolated, localized view of their data flows, but typically unaware of flows of external data sources, are now able to share a common picture of the data quality, logical connectivity and timeliness of the operational data flow among the battlespace capabilities. SMACQ provides access to simple traffic colour-coded indicators on the systems and services they use, via toggle-able geographical overlays, to improve their situational awareness and trust in the data they are sharing and receiving, so they can be more assured in how they use that data.
- OPS Service Management and Control, SMACQ provides up-to-date web access to the same shared common picture that the war fighters are seeing, with more detailed assessments of the data and connectivity quality indicators, enabling smarter, improved and shared means of monitoring, reporting on connectivity and data quality from source to consumer, to identify, understand and troubleshoot issues in a timely manner.

Service Features: According to the Bi-SC Operational Requirements for the NATO Common Operational Picture (COP), if the source quality of information data is available, then this shall be accessible to COP users.

SMACQ Application Service provides the following three enhancements to the NATO Common Operational Picture (COP) and Recognized Pictures (RPs) through a toggle-able geo-graphical overlay to the COP/RPs accessible via standardized interfaces (e.g. NVG, KML):

- Source Quality – SMACQ provides knowledge about the source quality, based on Standards-compliance, and potential degradation of the quality for various data flows. For example, the quality of tracks and/or messages generated by a source could be indicated by traffic-light colour-coded dots overlaid on the reported tracks and sources.

- Source Activity – SMACQ provides knowledge about the source activity and how much time had elapsed since that source reported on particular tracks. This is indicated by traffic-light colour-coded lines linking the reported tracks to the sources.
- Source Connectivity – from analysing the data flows from multiple points, the information about a source's logical connectivity, from source to consumer(s), can be inferred and/or extracted, and this information made available to the COP. The source connectivity per source are provided as lines connecting the monitored points from source to consumer(s).
- Data Timeliness – by analysing the data flow activity at each monitored point, the information about data timeliness is also made available to the COP. The data timeliness per connection are indicated by traffic-light colour-coded lines connecting each of the monitored points from source to consumer(s).

Service Flavours: The SMACQ Application Service can be offered as a single stand-alone decentralized application service or as a centralized hosted service.

- A centralized hosted SMACQ service can provide insight into an enterprise-level operational network, such as NATO Static Command, to monitor and assess data flows.
- A separate SMACQ application service may provide run-time support during missions and exercises or in a federated-environment, providing localized assessment of those networks, as needed.

Available on:

NATO Secret
Mission Domain
PAN
The Service may be available on other security domains upon a New Service Request.

Service Prerequisites:

WPS001 Managed Device Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A1012	NIRIS SYSTEM ADMINISTRATOR

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP013 Data-centric Information Services Gateway (DISG) Application Service

Service ID: APP013

Service Name: Data-centric Information Services Gateway (DISG) Application Service

Portfolio Group: Application Services

Service Description: The DISG (Data-centric Information Services Gateway) Application Service provides functional service proxies (FAS Proxy) that support Information Exchange Gateway (IEG) solutions to enable cross-domain exchange of operational data (e.g. Chat, TDLs, JISR, Air, Land, and Maritime). DISG can support IEG-B and IEG-C scenarios (NATO Secret to NATO-Nation Secret enclave, and NATO Secret to NATO-led Mission Secret enclave [reference ADaTP-34 NC3TA Vol. 2 v7, 2005]), which are the most relevant for NATO and partner nations.

Value proposition: Effective operations require the exchange of a wide variety of data within and between Command and Control (C2) systems. The traditional approach to multi-security-domain networking, forbids most information flows crossing the boundary of the security domain. This restrictive approach results in serious limitations to the information exchange requirements among C2 entities. Cross security domain services mediate in any information exchange occurring between the different information domains and levels of classification. The DISG Application Service provides the user with the integration of both Tactical data Link and chat services between distinct security domains, while protecting information assets of the participants in a federated environment.

Service Features: The DISG Service is designed to extend an IEG for Core Services (such as email or web browsing) with extra functionality (in this case with Functional Services). The purpose of DISG are:

(1) Label – determine and mark the security classification of information passing the IEG, in order to ensure that the information reaches the intended audience,

(2) Sanitize the information that is intended to leave the security domain. This sanitization will happen according to rules, and it removes or modifies data contents in order to be able to release functional services data into another domain,

(3) Sign – ensure that data or its security classifications are not changed, by adding digital signatures to the data, when converting data to XML format,

(4) Verify and guard – ensure the validity of the data by verifying adherence of data to the applicable standards or STANAGs (e.g. STANAG 5516 for Link 16 or XMPP standard for JCHat) both when entering the IEG and when exiting it. Invalid data will not pass the IEG.

The DISG supports multiple formats and protocols, including within the Tactical Data Link (TDL), Message Text Format (MTF), and Chat (XMPP) domains.

(5) The Diode option is special use case for low to high traffic and provides a way to bridge networks all the way from UNCLASSIFIED to SECRET. It offers a unique

HTTP(S) interface to seamlessly integrate into existing infrastructure. It can also leverage DISG to support the full suite of DISG supported protocols.

The service includes the following activities:

• Support for Incidents and Service request

• Problem management

• Monitoring and Event management (if agreed with Customer and remote access is possible)

• Yearly software upgrade in line with the NCI Agency approved DISG version (A2SL).

Service Flavours:

- APP013-1 Product management: This is the product management for DISG.
- APP013-2A Standard connection – small (per site): connecting up to 5 sites.
- APP013-2B Standard connection – medium (per site): connecting 5-10 sites.
- APP013-2C Standard connection – large (per site): connecting 10+ sites.
- APP013-2D Diode (per site)
- APP013-2E Tailored (custom calculated)

Available on:

NATO Secret
Availability on any other security domain is TBC upon a New Service Request.

Service prerequisites:

SEC011 Gateway Security Service (If used in a Scenario C case)

Standard Service support levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: For the flavours/options where there is a defined unit of measure, a standard service cost is specified. For the Tailored option, the unit of measure is 1, the total of the service delivery cost for these flavours is charged in accordance with specifically arranged conditions of the service delivery.

APP014 NMRR-VMS Application Service

Service retired.

APP015 JCHAT Application Service

Service ID: APP015

Service Name: JChat Application Service

Portfolio Group: Application Services

Service Description: The JChat (Secure Joint Tactical Chat) Application Service provides the user with a federated chat network to allow near real-time communication, or semi-synchronously via text messages, between two users, ad-hoc groups and within persistent chat rooms.

Value Proposition: The JChat Application Service is a key component in facilitating military effectiveness. It enables passing of information, coordination of operations and support to collaborative decision making. The service focuses on time critical operations in order to prevent casualties and minimise reaction time.

Service Features: The JChat Application Service key features, include but are not limited to:

- Multi-party messaging service (ad-hoc and persistent chat rooms)
  - Within a mission network, chat applications are used in a similar manner to Combat Net Radio, allowing all-informed exchange of information within specific groups or chat rooms.
  - Chat rooms are used both informally, for staff level coordination and collaboration, and formally, for rapid all-informed reporting and tasking.
- One-to-one messaging service (chat sessions)
  - Presence and instant messaging (IM) defines a method by which a client or user can formally request establishment of a presence and instant messaging session.
  - The functionality of the JChat Application Services follow open standards and are set in conformance with the requirements in RFC 2779 (“Instant Messaging / Presence Protocol Requirements”).
- Roster service (contact list)
  - In JChat, a user's roster contains any number of specific contacts. A user's roster is stored by the user's server on the user's behalf so that the user can access roster information from any device.
  - Because the user's roster can contain confidential data, the JChat server restricts access to this data so that only authorized entities (typically limited to the account owner) are able to retrieve, modify, or delete it.
- Presence service (logged-on users)
  - The concept of presence refers to an entity's availability for communication over a network. At the most basic level, presence is a boolean "on/off" variable that signals whether an entity is available or unavailable for communication (the terms "online" and "offline" are also used).
  - In JChat, presence typically follows a "publish-subscribe" or "observer" pattern, wherein an entity sends presence to its server, and its server then broadcasts that information to all of the entity's contacts who have a subscription to the entity's presence. A client can establish a "presence session" at its server by sending initial presence, and where the presence session is terminated by sending unavailable presence.

Service Flavours:

- Single, standard version based on NCI Agency prototypes
- Single, standard version based on Commercial Off the Shelf (COTS) software
- Clustered dual-node multi IM domain version based on COTS software
- Single, deployable version for mobile units based on COTS software
- Cross-domain chat version based on NCI Agency prototypes

Available on:

NATO Secret
Mission Secret

Service Prerequisites:

WPS001 – Managed Device Service
SEC011 – Information Exchange Gateway

Standard Service support levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A9001	JChat User
A9003	JChat FAS Manager
A9004	JChat Openfire Server Administrator
A9005	JChat M-Link Server Administrator
A9006	JChat Combined Openfire Server and JChat Client Administrator
A9042	Combined Situational Awareness Functional Area Services for CTE/exercise

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP016 JTS/FAST Application Service

Service ID: APP016

Service Name: JTS/FAST Application Service

Portfolio Group: Application Services

Service Description: The JTS/FAST (Joint Targeting System/Flexible, Advanced C2 Services for NATO Time-Sensitive Targeting) Application Service provides the user with capabilities to provide integrated joint objective and effects-based targeting, campaign synchronisation, target development, target list management, target folder preparation, target imagery management and battle damage assessment.

Value Proposition: The JTS/FAST Application Service, used throughout all command levels in NATO (both static and deployed) as well as nationally by various nations, enables collaboration and the efficient and timely exchange of critical information in support of the Joint Targeting process Furthermore this service is designed to aid tracking and prosecuting of Time-Sensitive Targeting (TSTs).

Service Features: The JTS/FAST Application Service contains two main end user modules, with distinct features:

- JTS features:
    - Deliberate Targeting
    - Kinetic and Non-Kinetic Targeting
    - Effects-Based Targeting (JFX)
    - High Value Individual (HVI)
    - Target Development
    - Target Folder Preparation
    - Objective Management
    - Target List Management
    - Target Nomination Process
    - Target Media Management
    - Weaponing Solutions
    - Battle Damage Assessment (BDA)
    - Campaign Synchronization
    - ATO Planning Cycle
- FAST features:
    - Dynamic Targeting (DT)
    - Time-Sensitive Targeting (TST)
    - Integrated Chat capability
    - Integrated Map functions
    - Network-enabled, real-time coordination

Service Flavours: The service is available as the following flavours**.**

JTS/FAST Software – includes all JTS/FAST software components and documentation to have either a full JTS/FAST site (server and clients) or JTS/FAST client workstations which would be able to remotely connect to a full JTS/FAST site.

JTS/FAST Capability – includes the JTS/FAST software, documentation, platform and database binaries for building a full JTS/FAST system with the full set of functionality provided by the JTS/FAST server and client.

Available on:

NATO Secret
Availability on any other security domain is TBC upon a New Service Request

Service Prerequisites:

WPS001 Managed Device Service

Standard Service Support Levels: The NCI Agency offers service support packages for AirC2 applications and systems defined by the provided service levels and set of support tasks. The support tasks can be all or a subset of the following group of tasks:

- XAA First Line Support
- XAB Second Line Support
- XGM Third Line Support
- XAD Data and Document Provisioning
- XDC Contract and License management
- XBC Installation
- XCC Interoperability Management
- XDD Product Maintenance
- XGC Security
- XGJ Obsolescence management
- XBB On-site maintenance
- XBD Site Support
- XFA Individual Technical training
- XGK Technical Manuals
- XED ILS management
- XGI Deployment of deployable equipment
- XCB System status and statistics
- XGF Database management and engineering
- XFB Support to OT&E and exercises
- XIC Platform and tools support

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Available NCI Academy Training not covered by service cost:

A1007	JTS/FAST System Administrator
A9008	Functional Area Service for dynamic and time-sensitive Targeting (FAST) User Course
A9011	Joint Targeting System (JTS) User
A9073	JTS/FAST Combined User Course

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

NATO Communications and Information Agency

APP017 Land C2 Application Service

Service ID: APP017

Service Name: Land C2 Application Service

Portfolio Group: Application Services

Service Description: The Land C2 (Command and Control) Application Service provides a suite of land command and control applications that support operational land staff in decision making and execution of missions, processes and tasks.

The Land C2 Application Service, through LC2IS (Land C2 Information System), delivers comprehensive situational awareness, battlespace management, sharing of information and interoperability within the land C2 domain and between other NATO functional services and national land C2 capabilities.

Value Proposition: The Land C2 Application Service offers a wide range of features to the user including shortened information-decision-action (IDA) cycles, inherent to command and control of mission execution. The service enables:

- Effective, efficient and accurate management of recognized ground picture (RGP);
- Enhanced battlespace management;
- Comprehensive NATO situational awareness;
- Support for operations planning and FRAGO production and message generation;
- Sharing of recognized ground picture, information and knowledge;
- Automated importing of recognized ground picture contributions and messages.

The proposed services ranges from the implementation of the Land C2 Application Service within headquarters through training and mentoring of operational and support personnel, as well as centralised resources for maintenance and (remote) support of the application service.

Service Features: The main service consists in the provision of the following service features:

- **Access to Land C2 Application Service** and related resources on selected networks and to the technical and functional knowledge base for self-support (requires access to the NCI Agency managed Operational Network).

- **Service Delivery Point (SDP) activation** provides on-site installation of one Land C2 Application Service instance and connection to all compatible and pre-configured local sources at time of installation.

- **SDP Centralised Management and Support** provides centralised management and maintenance of a SDP including assistance and advice to local support engineers. It includes routine upgrades and patches, as become available, in line with the approved baseline. For centralised management, remote administrator access is required.

- **SDP Remote Support** provides centralised assistance and advice to local support engineers who maintain the Land C2 Application Service SDP. It includes routine upgrades and patches, as become available in line with the approved baseline. This option is available when no remote administrator access is feasible or required

- **Incidents and Service Requests Management** provides centralised support to resolve incidents and/or address service requests via ITMS ticketing system to log, categorize and escalate if applicable. Response time and level of response in accordance with defined service level agreement.

Service Flavours: The service is available in multiple flavours:

APP017.1 LC2IS Single Node

APP017.2 LC2IS High Availability

APP017.3 SitaWare HQ Single Node

APP017.4 SitaWare HQ High Availability

LC2IS is nearing end-of-life, flavours APP017.1 and APP017.2 may be discontinued from 2026 Q1 onwards.

SitaWare HQ is the emerging capability for land C2; in 2025 flavours APP017.3 and APP017.4 will only be available for specific NCS entities.

Available On:

- NATO Secret;
- Mission Secret;
- Deployable CIS;
- The application service may be made available on other networks upon a new Customer Service Request.

Service Prerequisites:

- WPS001 Managed Device Service;
- Infrastructure and hosting platform compatible with the Land C2 Application Service requirements.

Standard Service Support Levels:

- **Service Availability Target:** 99.5% availability.
- **Service Restoration:** The standard service restoration period for a critical incident is 8 hours.

  N.B. Full priority resolution times and generic service priority assignment matrix will be adhered to in accordance with the defined service level agreement.

Available NCI Academy Training (not covered by service rate):

A0450	LC2IS End User (358)
A0451	LC2IS Information Management
A0452	LC2IS Train the Trainer End User

A9007	NATO Land Command and Control Information Services (LC2IS) System Administrator

Training for SitaWare HQ is under development.

Service Cost / Price: The unit of measure for the service is 1. The total of the service delivery cost is charged in accordance with specifically arranged conditions of the service delivery.

.

APP018 Maritime C2 Application Service

Service ID: APP018

Service Name: Maritime C2 Application Service

Portfolio Group: Application Services

Service Description: Maritime C2 Application Service is provided by utilising Maritime Command and Control Information System (MCCIS) , which processes maritime data received from multiple sources (e.g. Nations), builds the NATO Recognized Maritime Picture (RMP), and displays the RMP on map, and disseminates the RMP to Nations, NATO Commands and other command and control applications. The Maritime C2 Application Service provides the operational users with maritime operational data, exchanged in a multi-national environment through Over the Horizon Targeting (OTH-T)-GOLD and Allied Data Publication No 3 (ADatP-3) messages. The service provides the Waterspace Management (WSM) and Prevention of Mutual Interference capabilities for subsurface mission space management. The system is built around a dedicated hardware server, which runs a legacy operating system. Static and afloat NATO Commands as well as Nations who contribute to the RMP building and sharing process utilize MCCIS on the NSWAN.

Value Proposition: The Maritime C2 Application Service provides the user with management of Maritime C2 information. The Service supports planning, controlling and monitoring maritime operations, and makes the RMP available for NATO security operations. This enables maritime commanders and HQ staff to automatically receive, analyse, display, and manipulate Maritime C2 data and manage subsurface mission space while supporting more accurate, timely decisions.

Service Features: The Maritime C2 Application Service provides the user with network services (managing communication channels, integrated chat), Web Information Service Environment capabilities (WISE), access to maritime databases. The Maritime C2 Application Service features maritime operational data, including but not limited to, naval mission reporting, situational awareness, resource management and intelligence.

Service Flavours: The service is available as a single flavour.

Available on:

NATO Secret

Service Prerequisites:

WPS001 Managed Device Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A0270	NATO MCCIS Orientation & User
A0271	NATO MCCIS RMP Operator
A0273	NATO MCCIS Site Administrator
A0275	NATO MCCIS Waterspace Management
A0277	NATO MCCIS RMP Supervisor
A0602	Maritime FAS Pre-study (013)
A0603	MCCIS Pre-study (014)
A0609	MCCIS Advanced (031)

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP019 White Shipping Picture Application Service

Service ID: APP019

Service Name: White Shipping Picture Application Service

Portfolio Group: Application Services

Service Description: The White Shipping Picture Application Service provides the NATO Shipping Centre with the capability of monitoring the civilian maritime traffic by means of Automatic Identification System (AIS) data provided by MSSIS and commercial AIS data service. The service utilises Maritime Situational Awareness (MSA) application developed on Baseline for Rapid Iterative Transformational Experimentation (BRITE) infrastructure, which provides the user with a display and a set of analysis functions called Smart Agents. The AIS data is ingested into MSA-BRITE by means of an input controller software, which is derived from NIRIS. The White Shipping Picture Application Service is deployed at HQ MARCOM to support the NATO Shipping Centre and the Maritime Operations Centre in support of C2 of Maritime Operations.

Value Proposition: The White Shipping Picture Application Service provides the NATO Shipping Centre in MARCOM with the capabilities to build the White Shipping Picture, and feeds the relevant parts of this picture to the Recognised Maritime Picture (RMP) managed by the Maritime C2 Application Service.

Service Features: The White Shipping Picture Application Service builds the White Shipping Picture, provides analysis tools, and contributes to the RMP. This service features:

- Receiving AIS data from external sources with flow control;
- Processing the data to build White Shipping Picture;
- Displaying the White Shipping Picture on a map and also in tabular form;
- Providing automatic anomaly detection by means of smart agents;
- Ingesting selected parts of the White Shipping Picture into the RMP.

Service Flavours: The service is available as a single flavour.

Available on:

NATO Secret
NATO Unclassified

Service prerequisites:

WPS001 – Managed Device Service

Standard Service support levels:

Service Availability[1] Target: 99.5% Availability

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP021 JOCWatch Application Service

Service ID: APP021

Service Name: JOCWatch Application Service

Portfolio Group: Application Services

Service Description: The JOCWatch (Joint Operations Centre Watch) Application Service provides the user with a web-based electronic event log. The JOCWatch Application Service provides support to Watch Keepers and Shift Directors within Operation Centres (CJOC, JOCs, etc.) to record and disseminate incident information in a standardised and structured manner. It also provides an audit trail (a legal log) of all incidents related to an operation.

Value Proposition: The JOCWatch Application Service offers a common web-based interface which allows Operations Centre staff to manage, analyse and publish information on incidents. Through provision of event-data for analysis of the battle-space this service enables greater situational awareness for decision makers from subordinate commands to their HQ.

Service Features: Functionally JOCWatch Application Service offers a web based interface to:

- Capture and publish incident information,
- RSS Feed alerting of incident updates
- Search and audit capabilities,
- Compatibility with KML (show of incidents in Google Earth)
- NATO Vector Graphics web services (Map overlaying).
- Dashboard reporting (providing an immediate overviews of situations).
- Interoperability with multiple NATO and National Systems (e.g. LOGFAS, iGeoSIT, CC).

Service Flavours: The JOCWatch Application Service is in the following flavours:

APP021 Centralised offering

APP021F Federated offering: This service flavour provides federation support to NFS and Nations for authorization, configuration and troubleshooting of their connections to an JOCWATCH Service Delivery Point (identified as centralized NCS CoI servers). This flavour also encompasses Application changes triggered by federation requests and compensation for capacity increase required by the increasing demand on corresponding centralized infrastructure.

This service flavour ensures initialization and continuity of the COI interconnections between Nations & NFS with NCS. Troubleshooting beyond NATO Interconnection Point on the national or NFS side is not included in this service flavour.

- Management of technical connectivity to centralized NCS COI servers given the requester has authorization from SHAPE and the corresponding NCS party
- Troubleshooting on configuration of the connection to centralized NCS COI servers
- Application service delivery monitoring & corrective actions
- Application changes triggered by this federation request

- Compensation for capacity increase as per the increasing demand on corresponding NCS CoI servers

SME007 service is recommended to complement this flavour, would the Customer have connectivity in B2B mode. This is recommended for support beyond NIP.

Available on:

NATO Secret
Mission Secret

Federated flavour: NATO Secret

Service Prerequisites:

WPS001 Managed Device Service

For the Federated Flavour: Network connectivity for NIP interconnection with NATO centralized network (NS)

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A9033	JOCWatch User
A9034	JOCWatch Maintainer
A9035	JOCWatch Administrator
A9042	Combined Situational Awareness Functional Area Services for CTE/exercise

Service Cost / Price: The unit of measure for the Service is 1 for the centralised flavour. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

For the Federated flavour the unit of measure for the Service is per connection.

APP022 NCOP Application Service

Service ID: APP022

Service Name: NCOP Application Service

Portfolio Group: Application Services

Service Description: The NCOP (NATO Common Operational Picture) application provides operational user with a common view of the battle space. NCOP is interoperable with a large set of NATO and National Systems, collating and harmonizing authoritative information into Common Operational Pictures (COP) tailored for a mission or an area of interest, thus enabling a timely execution of operational users' processes (Battlespace Management, Logistics, Targeting, MEDEVAC, etc).

Furthermore, the NCOP Application Service also contributes to the Ballistic Missile Defense capability through integration of specific functions and interfaces for BMD.

Value proposition: The NCOP Application Service offers a wide range of support to entities willing to make permanent or temporary use of NCOP in their static and/or deployed environment. The proposed services ranges from the implementation of an NCOP instance through to corrective maintenance, including training and mentoring of operational and support personnel, as well as centralised resources and support for handling service degradation or interruption.

Service Features:

- **Access to NATO Common Operational Picture** application and related resources through the NCI Agency DML (under license agreement) and to technical and functional Knowledge base for self-support (requires access to the Agency managed Operational Network)
- **Service Delivery Point (SDP) activation** provides on-site installation of one NCOP instance and connection to all compatible and pre-configured local sources at time of installation. Includes training of up to 3 COP managers (see NCI Academy ref. A9047 for details) and access for users through the Activation of Service Access Point feature (1 unit is included) for a maximum of 3 SAP for the same SDP.
- **SDP Remote Support** provides centralised assistance and advice to local Support Engineers who maintain the NCOP SDP and includes up to one on-site upgrade in line with the approved baseline. By default, includes 12 tickets with a maximum response time of 5 business days. No remote administrator access required.
- **SDP Management** includes "SD Remote Support" and complements with a local footprint for technical support. Remote administrator access required.
- **Service Access Point (SAP) activation** provides configuration of on-site user access to an existing NCOP SDP for up to 24 users to consume a shared COP. It includes combined training from COP User through to COP Contributor for up to 24 users (see NCI Academy ref. A9054 for details), as well as knowledge transfer for 2 Support Engineers to act as first responder for Incidents and Service Requests and interface with the Agency Support.

- **SAP Remote Support** provides centralised assistance and advice to resolve incidents and/or address service requests via NATO/NCIA ITSM ticketing system to log, categorize and escalate if applicable. By default, includes 12 tickets per SAP. No remote power-user access required.
- **SAP Management** includes “SAP Remote Support” and complement with a local footprint for Functional/technical advice as well as technical liaison with the SDP management and assistance in recording and handling incidents and/or service requests via NATO/NCIA ITSM ticketing system. Remote power-user access required.

Service Flavours: The service is available with the following flavours:

APP022 Centralised

APP022 Federated: This service flavour provides federation support to NFS and Nations for authorization, configuration and troubleshooting of their connections to an NCOP Service Delivery Point (identified as centralized NCS CoI servers).

This flavour also encompasses Application changes triggered by federation requests and compensation for capacity increase required by the increasing demand on corresponding centralized infrastructure.
This service flavour ensures initialization and continuity of the COI interconnections between Nations & NFS with NCS. Troubleshooting beyond NATO Interconnection Point on the national or NFS side is not included in this service flavour. The service flavour offers:

- Management of technical connectivity to centralized NCS COI servers given the requester has authorization from SHAPE and the corresponding NCS party
- Troubleshooting on configuration of the connection to centralized NCS COI servers
- Application service delivery monitoring & corrective actions
- Application changes triggered by this federation request
- Compensation for capacity increase as per the increasing demand on corresponding NCS CoI servers

SME007 service is recommended to complement this flavour, would the Customer have connectivity in B2B mode. This is recommended for support beyond NIP.

Available on:

All NATO and National networks

Federated flavour: NATO Secret

Service prerequisites: Infrastructure compatible with the requirements of the NCOP application as described in the Release documentation.

For the Federated flavour: Network connectivity for NIP interconnection with NATO centralized network (NS).

Standard Service support levels:

Service Availability Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

Available NCI Academy Training not covered by service cost:

A9046	NATO Common Operational Picture (NCOP) User
A9047	NATO Common Operational Picture (NCOP) COP
A9048	NATO Common Operational Picture (NCOP) Combined User and COP
A9049	NATO Common Operational Picture (NCOP) FAS Administrator
A9050	NATO Common Operational Picture (NCOP) System Administrator
A9051	NATO Common Operational Picture (NCOP) Combined COP Manager and FAS Administrator
A9053	NATO Common Operational Picture (NCOP) Train the Trainer Operational User

Service Cost / Price: The unit of measure for the Service is 1 for the centralised flavour. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

For the Federated flavour the unit of measure for the Service is per connection.

APP023 NAMIS Application Service

Service ID: APP023

Service Name: NAMIS Application Service

Portfolio Group: Application Services

Service Description: NATO Automated Meteorological Information System (NAMIS) Application Service provides a sustained NATO Meteorological and Oceanographic (METOC) application functionality for the NATO. NAMIS Application Service provides direct weather support to NATO-led operations by providing coherent, comprehensive, and harmonised weather information and products throughout ACO activities.

Value Proposition: The NAMIS Application Service delivers METOc information to its users, principally within two Communities of Interest groups; MetOc and Ops Communities. NAMIS Application Service enables the user to access raw MetOc data and able to produce MetOc observations. Those can be used to support Exercise or Operation planning, Navigation, Natural Hazard Prevention/Analysis, Logistic Support Planning, Air/Missile Defence Operation planning/analysis, Weather Forecast Impact Analysis purposes. Users can also visualise all available MetOc products and data via NAMIS. Thus, interoperability of weather systems and other FAS is enabled.

Service Features: The NAMIS Application Service provides below listed features:

- Provision of Environmental Information Products,
  - MetOc Data Distribution System
- Meteorological Assessment,
  - visualization of forecasts,
  - visualization of observations,
  - visualization of value added products such as satellite images,
  - management of information on meteorological stations
- Tactical Specialist Tools,
  - Meteorological messages for CBRN (EDM and CDM),
  - Ballistic Wind Messages,
  - Color state and forecast trend for user selected airfields (METWATCH),
  - Products supporting parachute operations Mean Effective Dropping Wind (MEDW), Surface Wind and Gusts (SFG),
  - Theatre Crosswind Monitor, to monitor selected airfield for crosswind threshold,
  - Density Altitude calculator to verify conditions for use of air assets on the specific areas,
  - Graphical depiction of "Human Exposure", including Temperature-Humidity index (Heat Stress), Wind-Chill, Cold-Water Survival,
  - Night Illumination.
- Operational Planning Support (meteorological briefs in support of operations);
- Meteorological briefs in support of operations.

Service Flavours: The NAMIS Application Service is available as three flavours; namely:

- NAMIS X Premium; Superior license type providing full suite of full MetOc analysis tools
- NAMIS Basic; junior license type providing access to limited MetOc analysis capability
- NAMIS ‘NATO MetOc (NMD) Web Portal providing access to…MetOc information

Available on:

NATO Secret
NATO Unclassified
Mission Domains

Service Prerequisites:

WPS001 Managed Device Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP025 Naval Mine Warfare Support Application Service

Service ID: APP025

Service Name: Naval Mine Warfare Support Application Service

Portfolio Group: Application Services

Service Description: The Naval Mine Warfare Support Application Service consists of MCM EXPERT, which is a tool used for planning Naval Mine Counter Measure (MCM) operations to achieve user-specified level of clearance of maritime channels through uniform and non-uniform coverage according to the doctrine stipulated in STANAG 1454. The service is used on standalone computers at operational-level NATO sites and on board MCM vessels at tactical level.

Value Proposition: The Naval Mine Warfare Support Application Service offers the user a Graphical User Interface (GUI) for interactive planning of MCM operations. Based on the user inputs for a number of MCM operation types, MCM EXPERT provides the user a response in the form of a set of minesweeping or mine hunting tracks, with specific placement across the channel, and the clearance and remaining risk level achieved after completion of the given plan.

Service Features: The Naval Mine Warfare Support Application Service provides the ability to build Uniform and Non-Uniform MCM plans based on level of clearance, remaining risk, and Non-Uniform plans for time-constrained operations. Metrics of clearance, and remaining risk, achievable with the selected plan presented to the user.

Service Flavours: The service is available as a single flavour.

Available on:

NATO Secret

Service Prerequisites:

WPS001 Managed Device Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP026 Virtual Battle Simulation (VBS) Application Service

Service ID: APP026

Service Name: Virtual Battle Simulation (VBS) Application Service

Portfolio Group: Application Services

Service Description: The Virtual Battle Simulation (VBS) application service supports an exercise control organisation in maintaining a virtual situation of the battle space consistent in time and space at the level of detail of individual actors with a degree of realistic visualisation.

The VBS application is a commercial-off-the-shelf immersive training application used to simulate a real-time video stream. It functions as stand-alone or connected to the JCATS model.

Value Proposition: This application service supports exercise designers and control organisations in generating life-like visualizations of the relevant battlespace.

Service Features: The Virtual Battle Simulation (VBS) application service offers the following features:

- Creation and modification of a virtual scenario including terrain, systems and personnel. Activities of systems and personnel can be pre-planned and previewed.
- A player and controller mode to execute the scenario and act as one the parties or as the scenario manager.
- Video capture to mimic the behaviour of real-time optical or infra-red sensors.

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Secret

Service Prerequisites:

WPS001 Managed Device Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP027 NATO Nuclear C2 Reporting Application Service

The Service is classified. Further information is available upon request and relevant clearance.

APP028 NATO Nuclear Planning Application Service

The Service is classified. Further information is available upon request and relevant clearance.

APP029 Military Message Handling Application Service

Service ID: APP029

Service Name: Military Message Handling Application Service

Portfolio Group: Application Services

Service Description: Military Message Handling Application Service provides the user, in both static and deployed environments, with the capability of drafting, releasing and receiving military messages (ACP127). The service also delivers a reliable message storing and forwarding infrastructure, which provides intercommunication between NATO organisations, Maritime Broadcast systems and National ACP127 networks.

Value Proposition: Military Message Handling Application Service offers the customers:

- The intercommunication between NATO and National Military Organizations,
- The automatic distribution of incoming and outgoing formal military messages based on information within a message and rules following the operational and administrative procedure,
- A workflow capability to support the coordination of message preparation.

Service Features: The Military Message Handling Application Service offers the customers the formal messaging capability with elements featuring:

- Access Management,
- Alternate Recipients,
- Conversation Prohibition,
- Deferred Delivery,
- Delivery Notification,
- Distribution List Expansion,
- Latest Delivery and Message Security Labelling
- Quality of Service adjustments based on different message priorities (e.g. expediting higher priority messages)

Service Flavours: The Military Message Handling Application service is available in multiple flavours based on the required functionality:

Standard: Message reception only (through e-mail services).

Upon request (increased functionality):

Sending out:

- Desktop application need to be installed (AIMS);
- Addressing needs to be available;
- Release authority to be established;
- SMAs and routing need to be configured. This flavour will be upon request. Note: multiple SMAs to be supported can be installed upon request.

Serial ACP127 connections to National Gateways and Broadcast systems (with or without dual homing).

Serial connections to end point locations including the installation of a PCTTY (ACP127 protocol).

Complete AIFS system.

Available on:

NATO Secret
Mission Secret

Service Prerequisites:

WPS001 Managed Device Service
WPS012 E-mail Services

Standard Service Support Levels:

Service Availability Target: 99.0% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A0160	Allied Information Flow System (AIFS) Administrator
A0161	Allied Information Flow System (AIFS) Operator/Shift Supervisor

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP030 Tasker and Project Tracker Applications Service (TT+ and PITT)

Service ID: APP030

Service Name: Tasker and Project Tracker Applications Service (TT+ and PITT)

Portfolio Group: Application Services

Service Description: The Service provides information management capabilities for the tracking of organizational tasking activities and for the tracking of all Allied Operations and Missions (AOM) related project information. Provides the quickest path to delivery and is in line with organizational directive for leveraging enterprise-established tools, services and support. The Tasker Tracker Plus Flavour is interoperable with an existing Enterprise Document Management Application Service (APP031) and an existing NATO Information Portal Application Service (APP086), but also deployable as standalone Service

Value proposition: The Service offers a collaborative, efficient, highly configurable, and auditable tool for management of organizational tasking activities, thus improving situational awareness and overall business operations.

Service Features: The Service supports the following core functionalities (subject to the specific Service Flavours):

- Multi- user collaborative tasking
- Advanced Task Search Engine
- Sub-Tasking (including favourites)
- Reporting on Taskers by Office and Status
- Business Intelligence
- Traffic Light Monitoring System
- Integrated Document Management.

Service Flavours:

APP030-1: TT+ (Tasker Tracker Plus): Provides an Information Management capability for the tracking of the organisational tasking activities, such as raising, delegating, monitoring, and management of tasks. This Service Flavour is interoperable with an existing Enterprise Document Management Application Service (APP031) and an existing NATO Information Portal Service (APP086), but also deployable as standalone Service.

APP030-2: PITT (Project Implementation Tracking Tool): Provides the capability of tracking all Allied Operations and Missions (AOM) related project information, facilitates collaborative work, and establishes a coherency to the CUR management of all projects through a centralized approach, which support management boards and additional supporting services, such as search and a report centre.

Available on:

NATO Unclassified

NATO Restricted
NATO Secret
Mission Secret
NATO Partner Network (For NNHQ)

Service Prerequisites:

WPS002 Enterprise Identity Access Management Service
WPS003 Enterprise User License Service
PLT003 Web Hosting Service

Standard Service Support Levels:

Service Availability Target: 99%

Service Restoration Priority: P2.

The Standard Service support comprises the following activities:

- **Operation**: application monitoring, log management, batch jobs management, backup & restore, auditing, Service Requests fulfilment.
- **Corrective Maintenance**: diagnosis and removal of the causes and the effects of any malfunction affecting the Service.
- **Preventive Maintenance**: preventive actions needed to avoid future malfunctions.
- **Adaptive Maintenance**: adjustment of the Service in order to adapt to the minor changes of the sub system components (i.e. Operating System, Database Management System, Browser, SharePoint and SharePoint add-ons). Major changes of the sub system components shall be requested via dedicated projects.
- **Minor Perfective Maintenance**: development of up to one minor enhancement[1] of the Service per month[2] (only applicable to the TT+ Service Flavour). Development of up to one complex Business Intelligence (BI) report[3] per year (only applicable to the TT+ Service Flavour)

Available NCI Academy Training not covered by service cost:

A2536	Tasker Tracker + (TT+)
A2539	TT+ - Functional Administrator

Service Cost / Price: The unit of measure for the Service is “per user”. Different types of users are considered for the calculation of the price of the two Service Flavours, as per the following table:

[1] A “minor enhancement” is defined as a limited change of an existing functionality or the creation of a new functionality of the Service, that requires in total not more than 5 man days in order to be designed, developed and tested. All the enhancement requests shall be vetted and prioritized by the “Bi-SC IKM Change Management Board” before being developed.

[2] This activity will be paused during major implementation projects affecting the Service.

[3] A “complex BI report” is defined as as a report that requires in total not more than 15 man days in order to be designed, developed and tested. The report can fetch data from the Tasker Tracker Plus (APP030), but also from the Enterprise Document Management System (APP031) and the NATO Information Portal (APP086). All the requests for new reports shall be vetted and prioritized by the “Bi-SC IKM Change Management Board” before being developed.

Service Flavour	Definition of “user”
TT+	TT+ is designed for the general use by all the users of each customer, so the number of user will be assumed to be equal to the sum of the “NATO Peacetime Establishment (PE)” users plus the “NATO Non-Peacetime Establishment (NPE)” users.
PITT	Only the users authorized to access the PITT will be counted as “users”.

Each instance of the Service should be counted separately (so for example, if the same user is using two different instances of the Service on two different networks, the user should be counted twice).

The cost of the Service does not include the cost of all the underlying Service prerequisites.

The total amount of the Service delivery price is charged in accordance with specifically arranged conditions of the Service delivery.

APP031 Enterprise Document Management Application Service (EDMS)

Service ID: APP031

Service Name: Enterprise Document Management Application Service (EDMS)

Portfolio Group: Application Services

Service Description: The Service provides the collaborative information management capability for Document and Records Management, with functionalities for standardised document creation, management, storage and retrieval. This Service is interoperable with an existing Tasker Tracker Application Service (APP030) and an existing NATO Information Portal Application Service (APP086), but also deployable as standalone Service.

Value proposition: The Service offers the customers the benefit to easily access and maintain documented information by providing information access control, locating and retrieval of documentation and provisioning of storage, complying with NATO standards.

Service Features: The Service offers the user:

- Customizable organisational and data structures
- “Private” and “Public” document libraries
- Versioning
- Check in/check out functionality
- Search and browsing of documents
- Record Centre Workflow and Drop-Off library
- Alerting capability
- Access control
- Creation of documents by templates
- Document conversion into PDF files
- Distribution and archiving of documents, compatible with the NATO Archive
- Physical Media Management
- Optional integration with Tasker Tracker Plus (TT+) and NATO Information Portal (NIP).

Service Flavours: The service is available as a single flavour.

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret
NATO Partner network (For NNHQ)

Service prerequisites:

WPS002 Enterprise Identity Access Management Service

WPS003 Enterprise User License Service
PLT003 Web Hosting Service

Standard Service support levels:

Service Availability Target: 99%

Service Restoration Priority: P2.

The Standard Service support comprises the following activities:

- **Operation**: application monitoring, log management, batch jobs management, backup & restore, auditing, Service Requests fulfilment.
- **Corrective Maintenance**: diagnosis and removal of the causes and the effects of any malfunction affecting the Service.
- **Preventive Maintenance**: preventive actions needed to avoid future malfunctions
- **Adaptive Maintenance**: adjustment of the Service in order to adapt to the minor changes of the sub system components (i.e. Operating System, Database Management System, Browser, SharePoint and SharePoint add-ons). Major changes of the sub system components shall be requested via dedicated projects.
- **Minor Perfective Maintenance**: development of up to one minor enhancement[1] of the Service per month[2]. Development of up to one complex Business Intelligence (BI) report[3] per year.

Available NCI Academy Training not covered by service cost:

A2537	EDMS - Enterprise Document Management System User
A2538	EDMS - Functional Administrator

Service Cost / Price: The unit of measure for the Service is “per user”. Since the Service is designed for the general use by all the users of each customer, the number of user will be assumed to be equal to the sum of the “NATO Peacetime Establishment (PE)” users plus the “NATO Non-Peacetime Establishment (NPE)” users.

Each instance of the Service should be counted separately (so for example, if the same user is using two different instances of the Service on two different networks, the user should be counted twice).

The cost of the Service does not include the cost of all the underlying Service prerequisites.

The total amount of the Service delivery price is charged in accordance with specifically arranged conditions of the Service delivery.

[1] A “minor enhancement” is defined as a limited change of an existing functionality or the creation of a new functionality of the Service, that requires in total not more than 5 man days in order to be designed, developed and tested. All the enhancement requests shall be vetted and prioritized by the “Bi-SC IKM Change Management Board” before being developed.

[2] This activity will be paused during major implementation projects affecting the Service.

[3] A “complex BI report” is defined as as a report that requires in total not more than 15 man days in order to be designed, developed and tested. The report can fetch data from the Enterprise Document Management System (APP031), but also from the Tasker Tracker Plus (APP030) and the NATO Information Portal (APP086). All the requests for new reports shall be vetted and prioritized by the “Bi-SC IKM Change Management Board” before being developed.

APP032 Personnel Management Application Services

Service ID: APP032

Service Name: Personnel Management Application Service

Service Type: Customer Facing

Portfolio Group: Application Service

Service Status: Available

Service Description: The Personnel Management Application Service is supporting the Human Resource community by providing users with tools and systems for supporting day-to-day operational activities such as Personnel, Jobs, and Organization Management for the NATO static and deployed Command Structure. The Service enables the user to access, collect, store, manage, analyse, present, process, and disseminate human resource information.

Value Proposition: The Service offers the user improved accuracy, relevance, and timelines of information, thus supporting more efficient HR processes and procedures. Furthermore, it enables improvements for Manpower Modelling, Crisis Establishment (CE), and Crises Response Operations (CRO) by reducing analysis and reporting workloads and through the production of standardised executive summaries and reports. It also enables the usage of a single identity token for physical and logical access control, visual identification and entitlement tracking.

Service Features:

This service can be tailored by the customers selecting the required service features (applications and portals) only. Service features are grouped into service flavours as below:

- **Applications in scope of this Service - Service Flavours**

Flavour Personnel and Manpower Management System – APMS Application;

APMS is a highly configurable and modular software suite designed for military organisations consisting of four core areas: Post and Organizational management, Personnel Management, Manpower and Manning Reporting, and Billeting. APMS draws data from the full spectrum of existing sources, which is then exploited to provide Commanders and Staff with an aggregated, costed, synchronised and timely view of the full spectrum of military activity.

Flavour Establishment Review – ERT Application;

ERT application allows to perform regular changes to establishments and organizational details (i.e. Establishment review (approx. every 5 years), Units reviews (approx. every 3 years), Crisis Establishments change every 6 months, Individual Post Changes (many each year).

Note:
This Flavour requires APMS as a prerequisite;

Flavour Workflow Management System – Genpact Sequence Application;

Sequence application is a COTS component within APMS used to design, develop, maintain and execute HR business work-flows. Existing workflows: NSTEP processing, Out-processing, In-processing, Absence Management, Skills Self Certification.

Note:
This Flavour requires APMS as a prerequisite;

Flavour Card Identification and Security Management – AMIS Application;

AMIS is the NATO card management system authorized to provide unique NATO ID card for physical access for NATO personnel as well as encoding user and administrator certificates onto PIV (Personal Identity Verification) smart card for computer system authentication.

Note:
This Flavour requires APMS as a prerequisite;

Flavour Privileges and Immunities Management – NSTEP Application;

NSTEP is a tax-free privilege system allowing NATO AMIS ID card holders to receive, consume and track their privileges and entitlements offered by NATO host nations.

Note:
This Flavour requires AMIS as a prerequisite;

Flavour Installation Access Control System – NIACS Application;

NATO Installation Access Control System provides the capability to verify the validity of a NATO AMIS ID card as well as checking the access to a given installation or security area.

Note:
This Flavour requires AMIS as a prerequisite;

Flavour NATO Installation Access Control System Companion Applications;

Companion applications were designed to work together with the NIACS service in order to support fixed access points where wireless capabilities are limited while providing a minimal set of information to the operators.

Note:
This Flavour requires AMIS as a prerequisite;

Flavour ISIPS: Installation Visitor Management and Host Nation Support;

ISIPS allows Registration Offices to record and manage host nation specific personnel information as well as register vehicles with local authorities. The system allows reporting on relevant information focusing on site and host nation regulations. ISIPS allows Security forces and International Military Police to record visitors, visitors passes, vehicle visitors and link them with the sponsor information allowing them to create meaningful reports for longer periods of time.

Note:

This Flavour requires APMS as a prerequisite;

Flavour HR Portals:

- **Performance Management System – NPMS Application;**
  Performance Management System allows HR community to perform the Annual Performance Appraisal for NATO International Civilians, setting annual objectives and performing the need it mid-term and annual reviews.
- **HR Portals**

  HR community dashboards with relevant information for specific user groups:
  - HRDS Dashboard (NU/NS)
  - Commanders Dashboard (NU)
  - ERT Portal (NS)
  - HRDS Business Portal (NU/NS)
  - International Military Police (IMP) (NU)
  - TESSOC

Note:

This Flavour requires APMS as a prerequisite;

- **Activities in scope of this Service:**

  Service Management of entire service lifecycle including regular user communication;

  Supplier Management:
  - Management of the required 3rd party contracts (contract signature, extension or termination as required)
  - Monitor delivery of 3rd party services/goods;

  Application Management:
  - **New Capability Development:**
    - Requirements Analysis, Solution proposal, Cost estimation, Development (including SW changes with 3rd party vendors as required) and Assignment of changes into logical release packages;
  - **Incident Management**:

        - Issue Investigation and Resolution; Escalation of tickets to 3rd party supplier when required and follow up until their final resolution;
    - **Independent Verification & Validation:**
        - Change Configuration Proposal (CCP) Submission and Follow up;
    - **Deployment:**
        - Configuration & Reconfiguration;
        - Deploying & Release, and Patches Management;
    - **Operations:**
        - Operate and perform the required maintenance on the application servers and the underlying platform.
        - Operate and perform the required maintenance on the databases including backup, restore and replication.
        - KPI Monitoring
        - Maintenance of the related AD Components;
        - Set up and Maintenance required Reference/Test and Development environment in DEVOPS and make it available for the Senior User representatives.
        - Sequence Management;

Service Flavours:

The APMS is a core Flavour, while AMIS, ISIPS and HR Portals are extended flavours that can be added to meet specific customer needs.

Available on: NU, NS, and RSM.

Service Prerequisites:

WPS001 Managed Device Service
WPS002 Enterprise Identity Access Management Service
WPS008 Enterprise Service Operations Centre Service
SEC015 Security Certificate Service
LEG008 Local Other Service

Standard Service Support Levels:

Service Availability[1] Target: 99.5%

Service Restoration: for NCS customers, the restoration priority will be as specified in centralised or local service level agreement.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price:

The cost is calculated **per Flavour per Number of Posts**. The price details available in the Service Rates document.

[1] The minimum “Monthly Uptime Percentage” for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP033 INTEL FS Application Service

Service ID: APP033

Service Name: INTEL FS Application Service

Portfolio Group: Application Services

Service Description: The Intel FS (Intelligence Functional Service) Application Service provides an integrated, robust and flexible capability supporting a suite of services available throughout the Bi-Strategic Command (Bi-SC) Automated Information System (AIS) to support the direction, collection, processing, and dissemination of intelligence in a timely and responsive manner in accordance with NATO policy, doctrine and guidance.

Value Proposition: Intel FS Application Service provides the NATO Intelligence Community with a capability that enables the following operational benefits:

- Sharing of intelligence services and data across NATO at all levels of command.
- Manage the direction, collection, processing, and dissemination of intelligence requirements.
- Enhance the dissemination of intelligence with Nations and other domains.
- Enhanced analysis and exploitation capabilities.
- Manage posting and publication of intelligence products.
- Information exchange supporting situational awareness, common operational picture and targeting.
- Support the management of the intelligence processes.
- Provide search and analytical capabilities to retrieve/analyse intelligence information.
- Support the generation and the management of Intelligence Information.
- Provide specialised functionalities in support of specific domains (imagery, local employee personnel, and battlespace objects).
- Provide intelligence collaboration and synchronisation mechanisms to share intelligence across NATO according to Communities of Interest.
- Support interoperability with external systems.
- Manage Users and Permissions.
- Support all operational mission types.

Service Features: The INTEL FS Application Service is comprised of the following features that combined support an overall intelligence cycle:

- Intelligence Direction (Request For Information (RFI) and Intelligence Requirement Management).
- Intelligence Search, and Analysis.
- Intelligence Processing – creation/management of intelligence products such as Battle Space Objects (BSO) and Intelligence Surveillance Reconnaissance products (ISR Products).
- Intelligence Management.
    - Maintenance of Intelligence products.

- Intelligence Dissemination.
    - Dissemination of intelligence products to the intended recipients.

Service Flavours: The INTEL FS Application Service can be fully customized and provided with different components enabled/disabled: LEP, RFI, Imagery, ASAS products, RSS, Administration, Domain Value management, CSD, etc.

Available on:

NATO Secret
Mission Secret

Service Prerequisites:

WPS001 Managed Device Service
APP055 Core GIS Geospatial Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A9026	Intelligence Functional Service (INTEL-FS) Basic User
A9027	Intelligence Functional Service (INTEL-FS) Battle Space Objects (BSO)
A9032	Intelligence Functional Service (INTEL-FS) Organisational Node Administration (ONA)
A9044	NATO Intelligence Functional Areas Services Training (NIFST)
A9061	Intelligence Functional Service (INTEL-FS) Intelligence Request Management
A9064	Intelligence Functional Service (INTEL-FS) System Administrator

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP034 Integrated Engineering Management (IEMS) Application Service

Service ID: APP034

Service Name: Integrated Engineering Management (IEMS) Application Service

Portfolio Group: Application Services

Service Description: The Integrated Engineer Management System (IEMS) Application Service is an integrated asset management tool, which provides operation, support, maintenance and infrastructure management functionalities.

Value Proposition: The IEMS Application Service enables the user to support the maintenance of the SHAPE Infrastructure within accepted and agreed response times as per SHAPE' requirements. In addition, this application enables infrastructure project management, supports material management and SHAPE property disposal business processes.

Service Features: The IEMS Application Service offers a modular approach in support of the SHAPE Base Support Group within one single centralized database:

- Project Management
- Buildings Management
- Warehouse Management
- Budget Management
- Budget Long Range
- Reimbursable Customers Management
- Bunker Management
- Capital Items Management
- Non-expendable Items Management
- Utilities Consumption Management
- PWL Personnel Management
- Timekeeping Management
- Fire Brigade Management
- Proposal Disposal Office Management

Service Flavours: The IEMS Application Service is available as a single offering.

Available on:

NATO Unclassified
The Service may be available on other security domains upon a New Service Request.

Service Prerequisites:

WPS001 Managed Device Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP035 eLeave Application Service

Service ID: APP035

Service Name: eLeave Application Service

Portfolio Group: Application Services

Service Description: The eLeave Application Service provides an organisation with an online environment, which allows it to effectively and easily manage and administer all Human Resources leave related activities in an automated and standardized manner.

Value Proposition: The eLeave application service provides a fully automated system, which supports the organization's HR leave processes. In doing so it delivers a standardized, accurate and paperless online environment in which employees, managers and Human Resources administrators can easily and efficiently manage leave activities; i.e. : "leave requests", "approval / rejection", "leave balances & statuses", …. As such it covers all the process steps; from leave submission to the eventual and final approval or rejection. The implementation of such a system greatly reduces the time and effort spent on the management and administration of all leave related activities and processes. Moreover, the e-leave IT system provides standardization across all HR leave activities. It should be noted, that it has been developed fully in line with NATO's HR processes, activities and business rules.

Service Features: The eLeave Application Service allows users, i.e. staff members, to request all types of leave (Annual Leave, Home Leave, Special Leave for Private Reasons, Special Leave on Marriage, Special Leave for Maternity and Paternity, Long Service Leave, Leave for Training, Leave for Military Service or Training and Unpaid Leave). The Service can also be used to report absence for health reasons (Sick Leave). In addition the service provides:

- Leave record for each staff member, including leave balances and home leave entitlements
- Automatic calculation of leave days (based on official holidays per duty location)
- Automatic e-mail notifications and tasks for approval
- Attachments (for sick leave certificates, etc.)
- Creation of calendar appointments from leave requests
- Personal detailed leave overviews for the staff members
- Reports for managers at various organizational levels
- Versioning of all leave data
- Archiving of previous years' requests
- Consideration of Annual leave cut-off dates in calculations
- Recording and parking of next year's leave to be processed by the end of the year

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified

Service Prerequisites:

WPS001 Managed Device Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period is 8 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is Per Database.

APP036 Finance (FinS) Application Service

Service ID: APP036

Service Name: FinS Application Service

Portfolio Group: Application Services

Service Description: FinS provides the user with an Enterprise Resource Planning (ERP) system (based on the Oracle E-Business Suite Commercial Off-The-Shelf software and some extensions (iTravel)) with capabilities to perform streamlined budget execution, accounting, procurement, payments, and travel processes. It allows the customer to be compliant with NATO Financial Regulations (NFRs), Procurement Directives and International Public Sector Accounting Standards (IPSAS).

The FinS Application Service provides O&M support for existing FinS implementations.

Value proposition: FinS offers the user greater transparency, flexibility, control and auditability over allocated and delegated budgets, thus facilitating NATO Strategic Commands, NATO Military Commands, NATO Agencies and other NATO Organizations focusing on their core business.

Service Features: FinS provides the following functional features:

- General Ledger;
- Accounts Payable;
- Accounts Receivable;
- Cash Management;
- Fixed Assets;
- Purchasing;
- Advanced Procurement (iProcurement, Procurement Contacts, Service Procurement);
- Travel Management (Travel Requests and Travel Claims);

FinS consists out of the following elements:

- FinS Operations: Daily management of hardware and software;
- FinS Incident and Problem Management;
- FinS Change Management: Change management in coordination with concerned stakeholders;
- FinS Training.

Service Flavours: The service is available as a single flavour, with available specific configurations.

Available on:

NATO Unclassified
NATO Restricted

Service prerequisites:

This service provides O&M support only. An implementation project, possibly including the procurement of software licenses, is a prerequisite.

WPS001 – Managed Device Service

Standard Service support levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

NATO OTAN

NATO Communications and Information Agency NCI AGENCY

APP037 Employee Performance Management Application Service

Service ID: APP037

Service Name: Employee Performance Management Application Service

Portfolio Group: Application Services

Service Description: The Employee Performance Management Application provides a web-enabled platform which allows stakeholders to assess employee performance through goal-setting and tracking, customizable review forms and scales, 360 degree feedback gathered from peers, competency tracking, and more. The application supports the performance management processes and activities which ensure that goals are consistently met in and efficient and effective manner.

Value Proposition: The Employee Performance Management service provides a strategic and integrated approach to increase the effectiveness of the organization by improving the performance of the people by developing the capabilities of teams and individual contributors. Furthermore this service enables:

- Greater transparency in the performance management process.
- Improved (regular) feedback for workforce.
- Encourages professional development.
- Get employees involved in their own progression.

Service Features: The Employee Performance Management Service provides the following features:

- Ad Hoc Reviews
- Alerts / reminders
- Appraisal History Tracking
- Cascading Goals
- Competency Tracking
- Custom Rating Scales
- Goal Setting and Tracking
- Individual Development Plans
- Self Service Portal
- Performance appraisals
- Integrated reporting features (PDF, online)
- Support for review cycles (configurable)
- Notifications via email
- Performance Management Dashboard
- Reporting / Status reports

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Restricted

Service Prerequisites:

WPS001 Managed Device Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period is 8 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP038 NATO Talent Acquisition Application Service

Service ID: APP038

Service Name: NATO Talent Acquisition Application Service

Portfolio Group: Application Services

Service Description: The NATO Talent Acquisition Application Service provides the customer with a modern, fully electronic capability to effectively and efficiently support recruitment campaign in line with NATO directives. This application supports the recruitment process from vacancy posting, video interviews, to successful candidate selection and onboarding for civilian personnel and various types of temporary workers at the NATO International Staff Centre, NATO International Military Staff, NCI Agency and NATO Alliance Ground Surveillance Management Agency.

Value Proposition: The NATO Talent Acquisition Application Service drives a significant reduction in cost for the execution of a recruitment campaign and seriously improves operational efficiency and quality results through the use of the application. This is achieved through increased automation of tasks as it accelerates the recruitment campaign. The application offers automated workflows and a single point to access the web-based front end for the applicants and the specialized application frontend and backend for the hiring managers and hiring officials. The use of the application enables effective, efficient, quality, faster and less-costly management of recruitment campaigns. Through its introduction, the application eliminated the need to print and distribute a large number of documents for the various stakeholders involved in the recruitment process. As the capability is built on one single database instance, but with built-in data segregation for each NATO entity, it allows each organization to remain in control of its own recruitment campaigns but also for the HR officials to share data and knowledge about candidate application history as needed. Additionally this service, through its search and apply functionalities, offers the applicant a greater recruitment experience.

Furthermore, this application increases NATO's image and branding as an employer trough the presentation of vacancies to a larger number of NATO bodies onto the same online recruitment platform and in the improvement of results, through attracting a wider range of active and passive candidates.

Service Features: The NATO Talent Acquisition Application Service offers the user recruitment campaigns; online job-boards; collection and management of applications; asynchronous video interviews, recruitment screening and evaluation tools, together supporting candidate selection and store and share of application histories.

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified

Service Prerequisites:

WPS001 Managed Device Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP039 P3SM and Workflow Application Service

Service ID: APP039

Service Name: P3SM and Workflow Application Service

Service Type: Supporting Service

Portfolio Group: Application Services

Service Status: Available

Service Description: The P3SM Application Service provides the user with Portfolio, Program, Project and Service Management capabilities to support the creation and execution of related processes and activities. The P3SM Application Service provides project start-up/planning/baselining/execution/control/collaboration, resource management, time accounting and reporting.

The Workflow Application Service provides the platform for all internal agency processes to be automated and digitised via web-based interfaces. The Workflow Application Service is responsible for automating and supporting a growing catalogue of core agency processes such as: Business Intake, Workforce Planning, Business Execution Planning and IIT Requirements Collection.

Value Proposition: The P3SM Application Service enables the enforcement of common project management procedures, data centralization and improved accuracy and control to project progress, expenses, resource management, execution & control and reporting. Furthermore, projects utilizing the P3SM Application Service benefit from easier redirection of resources to meet project demand and real-time monitoring of project performance.

The Workflow Application Service ensures internal agency processes are executed efficiently. The service removes manual process bottlenecks, reduces the burden of repetitive and time-consuming tasks from staff whilst also drastically improving data-quality and accurate process auditing and reporting.

Service Features:

- Project Execution and Control; Efficient execution of project controls towards effort and cost;
- Time Accounting System; allows project staff resources to report project/non-project activities and time spent;
- Project Collaboration; based upon SharePoint technology enables store/share/act on projected related information (documents, issues, risks).
- Automation of internal processes; Potential for any internal process, regardless of complexity, to be digitised.
- Workflow management; Allows process owners to administer and configure their own applications
- Data-Management; a bonus feature of the workflow platform is the ability to create web-based data-management tools
- Reporting; Configurable reporting functionality

Service Flavours: The Service is available in two flavours; The P3SM application flavour and the Workflow Application flavour.

Available on:

NATO Restricted

Service Prerequisites:

WPS001 Managed Device Service

PLT003 Web Hosting Service

PLT006 Database Administration Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A3000	PRINCE2 Foundation & Practitioner Certification Exam Preparation
A3001	MSP Practitioner Certification Exam Prep
A3002	Project Management Professional (PMP) Exam Prep
A3019	Microsoft Project Introduction
A3028	Project Management Training: Skills for Success
A3043	Agile Project Management Training for Practitioner & Foundation Certification

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP040 Enterprise Asset Management Application Service

Service ID: APP040

Service Name: Enterprise Asset Management Application Service

Portfolio Group: Application Services

Service Description: The Enterprise Asset Management Application Service provides an ERP system based on Oracle E-Business Suite Commercial Off-The-Shelf Software, the capabilities of which are to collect, process, present and distribute consolidated information of assets, from a lifecycle perspective (acquisition to disposal). This service supports the centralized management of assets and is technically integrated within the centralized NATO Automated Financial System (CNAFS Application Service) to drive better visibility on reporting, decision-making, sustainable financial discipline, regulatory compliance (Inventory IPSAS 12), data integrity, optimized and efficient asset management processes. The Service provides the capabilities for operating Logistics in compliance with the Property Accounting Directives ACE 60-80 and the NCIA 'Under Construction Successor for the superseded NCSA OSI A-16-04.

Value proposition: The Enterprise Asset Management Application Service offers centrally managed Inventory and Order Management capabilities, with delegation of specific operational tasks to the local CSU's, integrated with already existing procurement and finance capabilities to drive efficiencies in the lifecycle of asset management. Furthermore, amongst other benefits, utilizing the Inventory/Asset Management Application Service facilitates easier redirection of asset resources as well as improving the operating costs by avoiding duplicated procurement and rationalizing inventory and assets including traceability.

Service Features: The Enterprise Asset Management Application Service offers the following features:

- Inventory Management (Warehouse Configuration Management, Asset Receiving, Creation and Labelling, Stock Availability Planning); Item management, asset movement, physical inventory and periodical cycle counting, inventory replenishment, reporting, quantity and value management.
- Order Management; customer account / CisPOC(MRAH) Assignment / custodian / shipping / delivery addresses management, internal/external.
- Asset Cost Accounting; asset valuation/weighted average cost (WAC) calculation, inventory accounting/reconciliation and auditing.
- Approval Hierarchy along with automatic notifications defined in the system also ensures control and visibility of Asset Procurement and movements.
- Auditing capabilities inherently present in the system can be used to fulfil internal/external checks and also for KPI's for any performance improvements.

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified

NATO Restricted

Service Prerequisites:

WPS001 Managed Device Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP041 Logistics Functional Area Services (LOGFAS) Application Service

Service ID: APP041

Service Name: Logistics Functional Area Services (LOGFAS) Application Service

Portfolio Group: Application Services

Service Description: The LOGFAS Application Service enables the user to collect, store, manage, analyse, present and distribute deployment and sustainment, host nation support and military engineering information during NATO operational planning and execution. LOGFAS User Community includes Logistics, Movement and Transportation, Host Nation Support and Infrastructure & Engineering functional domains.

Value proposition: The standardization of logistics data and data formats and their timely exchange is the key to the success of complex logistics operations, especially to facilitate the coordination for deployment and sustainment of forces from multiple nations, with limited logistic assets and infrastructure and engineering capabilities. LOGFAS addresses the requirement to minimize the planning time for NATO deployments and to maximize the capability for rapid exchange of the associated plans, reports and other information to enable orderly flow of movements into, from and within theatre. It supports informed decision making.

Service Features: The LOGFAS Application Service is comprised of multiple modules, these are:

- ADAMS/ADAMS Web; Allied Deployment and Movement Systems module supports multinational deployment planning through provision of deployment plan development, feasibility estimation and Host Nation Support Concept of Requirements.
- EVE/EVE Web; Effective Visible Execution provides monitoring of movement and transportation activities and provision for plan adjustments during execution. EVE Web enables movement visibility and transport request management.
- CORSOM; Coalition Reception, Staging and Onward Movement provides visualization and oversight of theatre movements, during both deployment, execution and sustainment operations.
- LOGREP; Logistics Reporting provides reporting capabilities in pre-approved and standardized formats as laid out in NATO reporting directives.
- SPM/SDM; Sustainment Planning Module provides calculation functionality to support sustainment requirements for operations.
- GEOMAN; provides geographical information on the facilities, unit holdings and transportation networks. GEOMAN is also used to manage the Host Nation Support Capability Catalogue (HNS CAPCAT).
- LDM; enables maintenance, reporting and import/export of information on force profiles and holdings, supplies, packaging, consumption rates, transportation assets, and planning data.
- LOGNET; LOGNET is the collaboration portal for the logistics community operating on both NATO Unclassified and NATO Secret platforms.

Service Flavours:

Server based application: two types of clients (Windows application and Web Client) and a PostgreSQL Database Server;

Standalone application: Windows application using local PostgreSQL Database

Collaboration web portal (LOGNET) on NS and on NU (accessible from the Internet).

Available on:

NATO Secret
Mission Secret
NATO Unclassified (LOGNET)

Service prerequisites:

WPS001 – Managed Device Service

Standard Service support levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A0220	Allied Deployment and Movements System (ADAMS) Staff Officer
A0222	Coalition Reception, Staging and Onward Movement (CORSOM) Operator
A0223	Effective Visible Execution (EVE) Operator
A0224	Allied Deployment and Movements System (ADAMS) Basic Operator
A0225	Allied Deployment and Movements System (ADAMS) Advanced Operator
A0226	Logistics Reporting (LOGREP) Operator
A0227	Logistics Reporting (LOGREP) Train the Trainer
A0251	Logistic Functional Areas Services (LOGFAS) Staff Officer
A0252	Effective Visible Execution (EVE) Manager
A0253	Sustainment Planning Module (SPM), Supply Distribution Model (SDM) Operator
A0254	Logistic Functional Area Services (LOGFAS) Fundamentals & Basic Data Operator
A0255	Logistic Functional Area Services (LOGFAS) System Administrator and Manager

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP043 Interactive Simulation Package (ISP) Application Service

Service ID: APP043

Service Name: Interactive Simulation Package (ISP) Application Service

Portfolio Group: Application Services

Service Description: The service provides a flexible, state-of-the-art solution to support the execution of air operations, which enables nations to simulate radar data in order to generate plot data to use it in a training and/or testing environment.

Value proposition: The service enables conduct of testing and exercises by providing necessary radar data.

Service Features: ISP enables generation of necessary data for execution of exercises for air operations, with particular focus at the NATO Integrated Air and Missile Defence System (NATINAMDS) community. More specifically, it enables:

- Modelling of airborne, sensor, and ECM exercise elements and to engineer scenarios by retrieval, positioning, manoeuvring, altering and manipulation of various elements via the graphical user interface;
- Performing of scenario management (retrieve, save, add, build, merge and delete);
- Performing of preview functions on the scenario;
- Execution and control of scenarios by starting, stopping, pausing, rewinding and forwarding the exercises;
- Activation and deactivation of radar sensors;
- Performing of interactive “real-time” changes, upon request, to alter the scenario during scenario execution;
- Providing of exercise support for flight plan printouts of selected missions and providing of the generation of flight plans, visible within the Multi AEGIS Site Emulator (MASE) system or any other system using the ADEXP flight plan message format for direct flight plan injection;
- Providing of realistic training for operational crews in the use of mechanical and electronic counter-measures (chaff simulation);
- Allow for the control of simulated fighter aircrafts using manoeuvrable targets

ISP is a standalone product, supported on Solaris, with the NISP configuration for the Solaris installation as preferred one. ISP provides input to the MASE system, but does not dependent on the MASE baseline version.

Service Flavours:

NCS-wide ISP software maintenance and in service support: (singleton service provided to SHAPE) Includes the development, testing, and documentation of maintenance releases of all ISP software components and the continuous support of the eligible user sites.

Available on:

NATO Secret

NATO Classified

Service prerequisites:

PLT013 (former APP051) NATO Integrated Secure Platform (NISP)

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

Monday to Thursday: 0600 to 2200 (CET)
Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number:

Belgium +32 65 44 3177
Netherlands +31 70 374 3177
Italy +39 081 721 3177
Germany +49 282 4978 3177
USA +1 757 747 3177
For NATO HQ +32 02 707 5858

Service Requests:

To request the APP043 service please complete the Customer Request Form and contact NCI Agency Demand Management. https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

Due to the nature of the ISP service (standalone, client-only software application, used for training simulation purposes often on unreachable non-production / non-NATO networks) no service availability monitoring KPIs are defined.
In case an SLA is established for ISP support the standard NCI Agency service support KPIs (response and restoration times) apply unless otherwise negotiated.

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions between NCIA and SHAPE on an annual basis.

APP045 SIGINT COINS Application Service

The Service is classified. Further information is available upon request and relevant clearance**.**

APP046 HMART Application Service

Service ID: APP046

Service Name: HMART Application Service

Portfolio Group: Application Services

Service Description: The Human Intelligence (HUMINT) and Counter Intelligence (CI) support service offers subject matter expertise (SME) support to the applications used by HUMINT and CI. The applications facilitate users to collect intelligence provided by human sources. It includes the systematic and controlled collection and exploitation of HUMINT/CI by interaction with human sources, objects, or individuals. HUMINT and CI activities involve safeguarding and exploitation of human sources, and efficient collection, reporting and analysis integrated within the overall intelligence environment to provide decision makers with timely and accurate information necessary for conducting successful military operations.

Value proposition: HMART consists of two separate but related modules that address the HUMINT requirements (HMART SD and HMART OM). The modules combined provide support to the HUMINT process for NATO lead operations ranging from:

- Securely managing the highly sensitive identities of human sources,
- Support to HUMINT mission planning.
- NATO HUMINT doctrine standards based report writing (AIntP-5).
- Workflow driven life cycles of reports providing the mechanism to improve the quality of reporting and ensure the proper sanitization of information.

HMART OM also embeds a module LEP (Locally Employed Personnel) that support the CI Vetting processes within operational theatres.

Service Features: HMART consists of three modules that serve different parts of HUMINT and CI operations.

HMART SD (Source management and de-confliction) – a stand-alone module running on secured and ruggedized laptops within NATO lead operations. The purpose of the module is to maintain information that could potentially reveal the identity of the source. The module has the following functionalities:

- Management of a dossiers of human sources
- De-confliction of human sources based on biographic and biometric characteristics.
  - Biometric comparison based on biometric modalities of face and finger print information.
  - Biographic (or heuristic) characteristics that are the basis for de-confliction other than biometrics. Eye colour, estimated year of birth, living location, weight, tribe and many other fields considered to identify possible duplicate sources.
- Secured exchange of source information within the J2X command structure.
- Powerful search functions to allow for analytical processing of source information. Structured searches based on metadata fields, geographically oriented search and unstructured full text search in order to quickly identify the human source coverage within an area of operation.

HMART OM (Online Module) – an online reporting module for HUMINT operations and support to HUMINT mission planning.

- Internal and external report writing based on NATO HUMINT doctrine (AIntP-5)
    - Fragmentation Order (FRAGO)
    - Debriefing Area Reconnaissance (DBA RECCE)
    - Contact Form
    - HUMINT Report
    - CI Report (CI)
    - Liaison Contact Report (CI)
- A workflow driven report life cycle that contributes to timely reporting and improved quality of reports produced.
- An operations (OPS) matrix used for HUMINT mission de-confliction at J2X level.
- Support to analytical processes. E.g. identify the operational value of a source based on information provided by a source.
- Interoperability with J2 for external reports (CI Report and HUMINT Report)
- A central repository for all HUMINT reporting containing historical reference data and supports data analysis.

LEP – an online module to support the Locally Employed Personnel vetting procedures.

- Management of a dossiers of LEP's, Screening files, addresses, employment etcetera.
- De-confliction of LEP's based on biographic and biometric characteristics.
    - Biometric comparison based on biometric modalities of face and finger print information.
    - Biographic characteristics that are the basis for de-confliction other than biometrics. Eye colour, estimated year of birth, living location, weight, tribe and many other fields considered to identify possible duplicate sources.

Sub-Services:

- HMART implementation, integration and customization.
- Operations and maintenance (HW and SW upgrade, annual biometric maintenance licences, release and change management, system administration, monitoring, etc.).
- Training of HMART users and administrators either at the NCI Agency, HUMINT Centre of Excellence (HCOE) or on-site.
- HMART support during the preparation and conduct of operations, exercises and experiments.
- Information gathering for technical and training support.

This service provides full or partial technical and training support in the HUMINT information gathering, process and design, and production of tailor made reports.

Service Flavours: HMART supports HUMINT/CI operations by two distinct operational modules.

HMART SD – deployed on stand-alone laptops to provide the best protection of the identities of human sources.

HMART OM – as a networked capability used within the J2X structure for reporting and support to HUMINT/CI mission planning.

LEP – as a networked capability used within the J2X structure for vetting locally employed personnel. Can be integrated within HMART OM.

Available on:

NATO Unclassified (Training and exercise only)
NATO Secret (HMART OM/LEP)
NATO Secret stand-alone (HMART SD)

Service prerequisites:

HMART SD

HMART SD is designed to run on stand-alone ruggedized laptops (TEMPEST level B) with hardware encrypted HDD when used for operational purposes.

HMART OM/LEP

HMART is a fully web based application that requires a server installation. Client machines only require a HTML5 compatible browser like Chrome, IE11 or MS Edge.

Standard Service support levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A9015	J2X Intelligence Systems

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP047 Allied Command Operations Open Source System (AOSS) Application Service

Service ID: APP047

Service Name: Allied Command Operations Open Source System (AOSS)

Portfolio Group: Application Services

Service Description: AOSS is a centralized web-based application that constantly collects open and subscribed source information from news agencies and Internet and transfers it in real time to the different networks within NATO. The core of AOSS uses the enormously powerful IDOL search engine from Hewlett-Packard, which allows AOSS to index a nearly unlimited amount of any type of documents and search them rapidly. Being a semantic engine, it offers “entity extraction” (i.e. it recognises persons, places, amounts, etc.) as well as multilingual automatic categorisation, highlighting, taxonomies, metadata extraction, clustering and a lot more.

Value Proposition: An estimated 80% of required information available for use in open sources for specific information vital for a deep analysis is available in newspapers, magazines, industry newsletters, television transcripts, and blogs. By using OSINT services, the Intel Analysts are able to get pertinent and essential information in the most effective way. Intel Analysts will find in AOSS the Political, Economic and Military Indicators and Trends they need to correlate with their findings, and updates on the classified side. Public Information Officers will use the watcher and report generation features to produce a daily Open Source compilation for their Commander-in-Chief. OSINT is unclassified and available, but link-crawling search engines like Google do not always access it. By researching various sources online, the OSINT service provides more information about what a company, individual, group, or country is up to, but it’s not always easily found. The use of OSINT has grown within the private sector as well as being a mainstay of the military and the intelligence services for years.

- **Uncovering**: Knowing who knows about the data and knowing where to look and we get the appropriate data are the key process which leverages distributed centres of expertise and archival knowledge.
- **Discrimination**: Careful discrimination between good and bad sources, current and outdated sources and relevant and irrelevant sources is part of the unique value of the process.
- **Refining**: *The most important value added* by the process is that of Refining; the final research report may be as short as a paragraph or a page.
- **Delivery**: The best intelligence/research in the world is useless if it cannot be delivered to the client in a timely fashion and in a format that can be easily understood.

Service Features: The AOSS Service offers the user:

- Real-time (24/7) indexation of feeds and images from external agencies (e.g. Reuters, Associated Press, Factiva (Dow Jones), Agence France Press, etc.) to make them available on the NATO networks.
- News feeds categorization by topics of interest.

- Web services for integration into other systems
- A simple and advanced search through the feeds and images.
- Watcher service: automatic search queries with notifications of new hints (also on mobile devices).
- Geocoding: the search results per each country visualised on the World Map.
- A cluster map tool to identify areas of high activities displaying data using a heat image.
- Statistics, trends and analysis of news feeds.
- Alerting: COI related content Email dispatching.
- A scrapbook metaphor to generate draft Intel products and briefs.

Service Flavours: The AOSS is available with different resources, and the following components are available separately:

- GeoTagger: produces GIS layers (KML and NVG 1.4 and 1.5)
- RSS feed provisioning (e.g. into SharePoint)
- Topic based Email notification service
- A set of web services that can be used without the AOSS front-end interface
  - Text highlighting web service
  - Category suggestion (meta tagging)
- Document Processing Service (DPS) powerful event based file handling service

Available on:

Internet facing
NATO Unclassified
NATO Secret
Mission Secret

Service Prerequisites:

WPS001 Managed Device Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A9039	Allied Command Europe Open Source System (AOSS)
A9044	NATO Intelligence Functional Areas Services Training (NIFST)

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

NATO OTAN
NATO Communications and Information Agency
NCI AGENCY

APP048 Analyst Notebook (ANB) Application Service

Service ID: APP048

Service Name: Analyst Notebook (ANB) Application Service

Portfolio Group: Application Services

Service Description: ANB offers a visual analysis environment designed to help analysts to turn large sets of disparate information into high-quality actionable intelligence and to help identify, predict, and prevent criminal, terrorist, and fraudulent activities. A flexible data acquisition approach allows analysts to more quickly collate both structured and unstructured information to help build a single, cohesive intelligence picture. The flexible data model and visualization environment coupled with a wide range of visual analysis tools help users build multiple views for detailed network, temporal, statistical, or geospatial analysis and reduce the time taken to identify key connections, networks, patterns and trends that may exist. The results gained from this detailed analysis may be shared via intuitive and visual briefing charts or visualizations that can be included in end intelligence products.

Value Proposition:

- Flexible data acquisition: rapidly import structured data, simplify the manual data entry process, connect to and query available data sources.
- Flexible data model and representation (environment that offers users flexibility in how data is modelled and visualized).
- Simple communication of complex data (intuitive and easy-to-follow visual briefing charts).
- Powerful analysis capabilities (wide range of analysis capabilities).
- Extensibility (see *Service Flavours)*.

Service Features: The Analyst Notebook (ANB) Service offers the user:

- Acquire data from disparate sources in order to piece together a coordinated picture that allows for an effective, more accurate analysis of available information.
- Establish key “who, what, where, when and why” information by analysing and visualizing data in multiple ways including association, temporal, geospatial, statistical, spreadsheet views and social network analysis, "list most connected" and "find connected networks".
- Identify connections, patterns, trends and key intelligence within a wide range of data types that might otherwise be missed.
- Discover duplicate information within data by leveraging intelligent semantic smart matching capabilities.
- Increase understanding of structure, hierarchy, method of operations and key individuals or groups within criminal, fraudulent and terrorist networks and the roles they may play, helping to guide future operational planning and resource allocation.
- Create clear and concise briefing charts to simplify complex data in support of more timely and accurate operational decision making.
- Simplify the communication of complex data to enable timely and accurate operational decision making.

- Capitalize on rapid deployment that delivers productivity gains quickly using a well-established visual analysis solution.

Service Flavours: The service is available as a single flavour. However, there is an extensive range of options available to extend further i2 Analyst's Notebook capabilities in order to provide even greater value to analysts and their wider organization. These come with additional costs:

- **Data Centric Analysis**—IBM i2 Analyst's Notebook Premium
- **Data Acquisition**—IBM i2 iBridge, IBM i2 Information Exchange for Analysis Search
- **Geospatial Analysis**—IBM i2 Analyst's Notebook Connector for ESRI
- **Unstructured Data Analysis**—IBM i2 Text Chart, IBM i2 Text Chart Auto Mark
- **Collaboration**—IBM i2 Analyze (via i2 Analyst's Notebook Premium), IBM i2 iBase
- **Extensibility**—IBM i2 Analyst's Notebook SDK

Available on:

NATO Unclassified
NATO Secret
Mission Secret (MS)

Service Prerequisites:

WPS001 Managed device service.

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A9014	NATO Use of IBM Analyst-s Notebook User

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP049 Integrated Command and Control (ICC) Application Service

Service ID: APP049

Service Name: Integrated Command and Control (ICC) Application Service

Portfolio Group: Application Service

Service Description: The NATO-wide Integrated Command and Control Software for Air Operations (ICC) is an integrated Command, Control, Communications and Intelligence/Information (C3I2) system that provides information management and decision support to NATO air operation activities during peacetime, exercise and crises. Currently, ICC provides functional support for the most critical Air C2 functions at the Joint Force Command, Air Command, and Combined Air Operations Centre levels as well as limited BMD functions. ICC consists of client and server applications, which can also be operated by different organisational elements. An organisational element can opt to utilize only ICC clients as standalone workstations (e.g. for parsing ATOs) or when allowed to connect to another element's ICC server for planning data and/or to a NIRIS server for RAP data.

Value Proposition: ICC provides capabilities for integrated planning, tasking, operations, information management and decision support to operational and tactical level air operations during peacetime, exercise, crisis and conflict. ICC also supports critical Air Command and Control (Air C2) functions at Air Component Command (ACC/JFACC) and Combined Air Operations Centre (CAOC) levels.

Service Features:

- Generation of Air Operations Directives (AOD)
- Generation of Airspace Control Orders (ACO)
- Generation of Air Tasking Orders (ATO)
- A capability for executing current operations at ACC/JFAC and CAOC units
- Automated status reporting
- Display of a Joint Common Operational Picture (COP) including the Recognized Air Picture (RAP) as provided from the Networked Interoperable (near) Real-time Information Services (NIRIS)
- Display of Shared Early Warning (SEW) information.
- TMD situational awareness and missile engagement (LSID)
- Replication of ICC related C2 data between sites
- Web-services interface to provide Air C2 information to interfacing systems

Service Flavours:

NCS-wide ICC software maintenance and in service support: (singleton service provided to SHAPE) Includes the development, testing, documentation and deployment of maintenance releases of all ICC software components and the continuous support of ICC sites throughout the NATO Command Structure (NCS).
ICC client: Provides the ICC Client application on WPS001 Managed Devices including local configuration to connect to (remote) ICC servers and other NATO FAS, version updates and continuous support.

ICC server: Provides an ICC Server on INF004 provided server infrastructure, including local configuration, version updates and continuous support.

Available on:

NATO Secret
Mission Secret

Note: APP049 is not provided on national security domains as the NCI Agency can only support as a service and guarantee service levels for ICC instances that reside on NATO networks. Nations can get ICC support for their national security domains via the SME007 service Bundle D.

Service Prerequisites:

WPS001 – Managed Devices. ICC clients require this service, which provides a standard NATO workstation connected to the NATO networks on which the ICC Client application can be deployed.

INF004 - Infrastructure Virtualization Services to provide the server instance (either physical or virtual) on which the ICC Server components can be deployed.

PLT013 (former APP051) NATO Integrated Secure Platform (NISP) Service. The ICC server service flavour requires the NISP service as NISP is the recommended platform for ICC server on NATO networks.

Oracle - The ICC Server support service requires a licenced Oracle database instance for ICC.

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

Monday to Thursday: 0600 to 2200 (CET)
Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 CET).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

Belgium +32 65 44 3177
Netherlands +31 70 374 3177
Italy +39 081 721 3177
Germany +49 282 4978 3177
USA +1 757 747 3177

For NATO HQ +32 02 707 5858

Service Requests:

To request the APP049 service please complete the Customer Request Form and contact NCI Agency Demand Management.
https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

The overall ICC availability will be measured as an aggregate of all the individual availabilities of the components listed below.

ICC functional component	Service Level Target (availability)	Performance threshold (determining when service is considered unavailable)
Airspace Management (ASMAN) (ACO generation)	99.5%	CRUD operations response < 5" for up to 25 concurrent users
Air Operations planning (SALTO) (ATO generation)	99.5%	CRUD operations response < 5" for up to 50 concurrent users
Mission (ATO) execution monitoring (MTOTE, OB TOTE,CADAP)	99.5%	CRUD operations response < 5" for up to 150 concurrent users
RAP Display	99.5%	delay<15" for up to 5,000 tracks
COP Display (Map)	99.5%	Responsive to map interaction (TBD)
BMD Situational Awareness (LSID, SEW)	99.5%	TBD
ICC DB replication (ICC Link)	99.5%	Heartbeat
ADATP3 message interface (MIMI) (ACCS-ICC interface)	99.5%	Heartbeat

KPIs implementation: ICC already contains some internal monitoring functionality. The necessary changes to expose the above availability KPIs are planned for implementation as part of the product roadmap.

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

> **N.B.** Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Available NCI Academy Training not covered by service cost:

A1000	Combined NISP ICC System Administrator (CNIC)
A1001	Windows ICC System Administrator (WICC)

A9009	Integrated Command and Control (ICC) Data Manager
A9010	Integrated Command and Control (ICC) User

Service Cost / Price: Unit of measure used for service quantification for each flavour can be found in the table below:

Service ID	Service Name	Service Flavour/Option	Service Unit of Measure
APP049	Integrated Command and Control (ICC) Application Service	NCS-wide ICC software maintenance and in service support	1
APP049	Integrated Command and Control (ICC) Application Service	ICC client	Per client
APP049	Integrated Command and Control (ICC) Application Service	ICC server	Per server

APP050 Air Command and Control Systems (ACCS) Application Service

Service ID: APP050

Service Name: Air Command and Control Systems (ACCS) Application Service

Portfolio Group: Application Services

Service Description: Air Command and Control System (ACCS) provides Air Command and Control (AirC2) and Ballistic Missile Defence (BMD) services through a modern and integrated system being deployed at various user sites. It enables seamless Air C2 and BMD operations across multiple ACCS locations.

The Air Command and Control System (ACCS) First Level of Operational Capability (LOC1) is deployed to operational units at the NATO Command Structure (NCS) and the NATO Force Structure (NFS) contributing to SACEUR's NATO Integrated Air and Missile Defence System (NATINAMDS). ACCS is comprised of a core software providing the main functionality, site adaptation and is installed and operated dedicated hardware and COTS software platform. The ACCS core software is configurable to build ACCS entity types which realise a specific operational capability at various levels of command. This includes the Combined Air Operations Centre (CAOC), Air Control Centre/RAP Production Centre/Sensor Fusion Post (ARS), the BMDOC build on TMD1 functionality and in the future, after implementation for the Addendum 3 System Adaptation, the Joint Force Air Command. A CAOC or an ARS entity may be static or deployable and a combined implementation of a CAOC and an ARS constitutes a CARS (Combined ARS).

Value Proposition: The value of ACCS is the integration of almost all relevant functions and external interfaces required for executing seamless Air C2 and (T)BMD) Operations within a network of ACCS sites at different level of command. Those functions can be installed at static sites as well as implemented as deployable or mobile site configurations.

Service Features:

The ACCS LOC1 covers the following Air C2 related operational functions:

- C2 Resource management including configuration planning, tasking and monitoring;
- Air Space Management including planning and utilization of the air space and mission preparation;
- Surveillance including Air Picture Production and related asset management;
- Air Mission Control including Air Policing Management, aircraft and SAM control;
- Force Management including allocation planning and tasking (A/C and SAM units);
- Air Traffic control including integration with civilian Air Traffic Control (ATC) centres and sensors.

ACCS TMD1 augments above ACCS operational functions to build (tactical) Ballistic Missile Defence (BMD) specific functionality utilized as the main system at the Ballistic Missile Defence Operations Centre (BMDOC). This (T)BMD specific functionality build by ACCS TMD1 covers Surveillance Operations, Sensor Management, Planning and Tasking, Engagement Operations, creation, visualization of a (T)BMD picture and dissemination to BMD sites.

Service Flavours: ACCS consists of several standardized entity types which are used in different combinations to build ACCS operational sites at different level of operational command.

As prerequisite for these flavours, centralised ACCS Core software maintenance is being executed and NCS wide In-Service-Support is provided to ACCS sites within the NCS. The ACCS Core software maintenance delivers site specific ACCS baseline and security updates is a pre-requisite for below service flavours offered to operational units:

OPS Level	Services
(D)ARS	The (deployable) ARS is a combination of the individual ACCS entities ACC, RPC and SFP. The Air Control Centre (ACC) executes air mission control within a dedicates area of operational responsibility (AOR): • Covers real-time (RT) battle management; • Performs air mission control for all types of manned air missions and SAM weapons; • Provides ATC services. The RAP Production Centre (RPC) enables air surveillance by producing and disseminating the Recognised Air Picture (RAP) data within its assigned AOR: • Receives land and maritime surface tracks and sub-surface tracks from external links and disseminates them to the ACCS users. • Manages its subordinate and allocated ACCS surveillance areas in accordance with orders and priorities received from the CAOC. The Sensor Fusion Post (SFP) contributes to air-surveillance by receiving data from various sensor sources and building a local air picture as basis for establishment and the maintenance of an RAP at the RPC: • Develops a local air picture (LAP) through the fusion of data from both active and passive sensors; • Reports on the status and performance of subordinate sensors; • Controls the sensor detection and responds to anti-radiation missile (ARM) threat and electronic counter-measures (ECM) activity.
(D)CAOC	The (deployable) CAOC is the entity in charge of the tasking of the assigned air assets, it:

	• Plans and conducts the tasking of air operations and C2 resources configuration within a designed AOR; • Supervises and monitors execution of tasking and analyses the results; • Coordinates with land, maritime and national forces as well as with other NATO and National agencies.
TMD1	ACCS TMD1 represents an entity specifically configured to provide the main C2 service for the BMD Operations Centre (BMDOC). It enables specific (T)BMD functions comprising: • Surveillance Operations, • Sensor Management, • Planning and Tasking, • Engagement Operations • Creation, visualization of a (T)BMD picture and • Dissemination of the (T)BMD specific picture BMD related sites.
ACCS Deployable Assets	ACCS deployable elements augments ACCS operational entities like and ARS or CAOC to become deployable or mobile. It comprises: • Deployable/Transportable Equipment; • Deployable active and passive Sensors; • Interfacing Equipment & CIS Security Boundary Protection; • Communication Equipment and • Deployment support packages and primary mission support equipment.

Available on:

NATO Secret

Service Prerequisites: ACCS requires a dedicated operating platform consisting of CIS hardware, communications, COTS Software ACCS functional software and ACCS operational data. Data exchange with external system and between ACCS sites requires to be protected through firewalls as well as security appliances realised by Application Layer Firewall or Boundary Protection Devices:

SEC022 – Application Layer Firewall for Sensors and Flight Plans (ALF-SFP) Security Service

- Mandatory for interfacing with:
    - Military and civilian sensors for receiving sensor data,
    - Military sensors for sensor control,
    - Civilian ATC centres for receiving ATC flight plans.

INF028 – ACCS Sensor Integration Module (ASIM) Service

- Optional for converting military and civilian legacy sensor data formats into an ACCS conform sensor data format.

APP054 - L16@29k Application Service

- Optional for utilizing the L16@29K system to exchange Link 16 (Platform D) data with other platforms on the same Link 16 network.

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

Monday to Thursday: 0600 to 2200 (CET)
sFriday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 CET).

Incident-problem / Service Request reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

Belgium +32 65 44 3177
Netherlands +31 70 374 3177
Italy +39 081 721 3177
Germany +49 282 4978 3177
USA +1 757 747 3177
For NATO HQ +32 02 707 5858

To request the APP050 service please complete the Customer Request Form and contact NCI Agency Demand Management.
https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

Service Flavour	Service Level Target (availability)
All ACCS entity types (ARS, COAC, TMD1)	99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Technical hotline can be activated through the CSD and would within 2 hrs, provide technical remote assistance 24/7**.**

Available NCI Academy Training not covered by service cost:

A1002	ACCS System Manager
A1003	ACCS Security Officer
A1004	ACCS Communication Manager
A1008	ACCS-ICC interface Administration
A1016	ACCS Data Manager

Service Cost / Price: The unit of measure for the Service is 1 for all service flavours. Service Initiation and In-Service-Support will be provided and charged in accordance with the scope and financial estimates developed and agreed through site specific Technical Agreements.

Service ID	Service Name	Service Flavour/Option	Service Unit of Measure
APP050	Air Command and Control Systems (ACCS) Application Service	NCS wide ACCS software baseline maintenance and In Service Support (ISS) for NCS sites	1
APP050	Air Command and Control Systems (ACCS) Application Service	(D)ARS	1
APP050	Air Command and Control Systems (ACCS) Application Service	(D)CAOC	1
APP050	Air Command and Control Systems (ACCS) Application Service	TMD1	1
APP050	Air Command and Control Systems (ACCS) Application Service	ACCS Deployable Assets	1

APP052 Air Situation Data Exchange (ASDE) Gateway Service

Service ID: APP052

Service Name: Air Situation Data Exchange (ASDE) Gateway

[Currently implemented by the NCIA's Application Layer Firewall for Link 1 (ALFL1) product]

Portfolio Group: Application Services

Service Description: The purpose of the Air Situation Data Exchange Gateway service is to:

- Provide an operationally available and security approved Application Layer Firewall for Link 1 that can:
  - Act as a Boundary Protection Device that provides Boundary Protection Services (BPS) in accordance with the self-protecting node principle to provide protection of the infrastructure and to mitigate risk introduced by interconnecting networks working with different security classifications, e.g. to protect the Link 1 interface of NATO CRC's from external Link 1 connections
  - Deliver Information Protection Services (IPS) to enforce the information release policies, preventing unauthorized and uncontrolled release of information, ensuring that only the information intended to be exchanged are effectively transmitted under a controlled, security monitored regime, e.g. to allow the controlled exchange of unclassified Link 1 data with partner nations.
- Provide release and deployment services (installation), by leading or supporting all activities required for properly fielding of baselines to existing or new sites. This includes, but are not limited to:
  - Site survey and collection of site-specific installation information
  - In-house installation, configuration and system testing
  - Shipping and asset management services
  - On-site installation, configuration and operational testing
  - On-site training for ASDE Site Manager and ASDE Site Technician(s).
- Provide in-Service Support, by offering continues support to sites using Application Layer Firewall for Link 1 that includes:
  - First, Second and Third Level Support
  - On-site maintenance
  - Site Support
- Provide Security Services, in order to maintain agreed security posture. This includes:
  - Continuous liaising with security authorities to monitor updates in relevant security policies and directives and to implement any changes required.

- To implement new security patches from underpinning systems, perform regression testing, and make updates and installation procedures available to all registered sites by releasing Technical Bulletins at the AirC2 Systems' support sites on Internet (NU) and NSWAN (NS).

Value proposition: The Air Situation Data Exchange Gateway Service ensures that the Application Layer Firewall for Link 1 can act as a boundary protection device for NATO Link 1 connections, and realize NATO requirements for a bi-directional exchange of a RAP between NATO and Partner Nations. The Multi-Level Security system manages the controlled and monitored exchange of air picture data between networks of different information security and management policies.

Service Features: When exchanging data the system can operate in two states:

1) Filtering State, when exchanging Air Situation Data between an AirC2 system on HIGH classification (NS or NC) and a system with LOW classification (NR or NU).
2) Symmetrical State, when exchanging Air Situation Data between two systems on NC or NS.

Filtering State: Allows the exchange of the Air Situation with a Partner Nation by sanitizing the Link 1 messages to a level of NATO Unclassified. The filtering state offers four distinct modes:

- Peacetime Operations Mode
- Exercise Operations Mode
- Crisis Response Operations Mode
- Article 5 Operations Mode

The operational modes will determine the set of filter rules the Application Layer Firewall for Link 1 will apply and includes a pre-defined set of functionality by implementing:

- Coordinate conversion: masking of the originator site positions by using an arbitrary, bi-laterally agreed Data Link Reference Point (DLRP);
- Geographic filtering: selection of information for data exchange based on geographical areas;
- Data/Message filtering: message and data field filtering for sensitive information;
- Validation: message frame validation (on receipt from PN only).
- The Application Layer Firewall for Link 1 security enforcing capability provides the following capability;
- Trusted computing base: verification of message fields filtering and message frame validation.

Symmetrical State: The symmetrical state operates interconnecting two entities operating on NC and NS classification levels. As the RAP is classified NC only, the dissemination between those two entities does not require data filtering but only frame validation, in order to ensure that only Link 1 messages are exchanged.

Supported configuration and Interface Standards:

The Application Layer Firewall for Link 1 supports both filtering mode and symmetrical mode. Regardless of the mode, the software and hardware requirements are identical and no change of hardware / software is required to alter the mode of operation. The mode of operation is in fact a configuration parameter to be controlled by the system administrator. The Application Layer Firewall for Link 1 implements the Tactical Data Link protocol Link 1 in accordance with STANAG 5501, edition 7.

The services currently installed is Application Layer Firewall for Link 1 version 4.0.1 and 5.0.0. These are NATO Baselines under the governance and Configuration Control of the AirC2 SC.

Service Flavours:

NCS-wide ALF-L1 product maintenance and in-service support: (singleton service provided to SHAPE) Includes the development, testing, documentation and deployment of maintenance releases of all ALF-L1 system components and the continuous support of the eligible ALF-L1 sites both in NATO and PNs.

ASDE Gateway National Instance: For national use of ALF-L1 to provide Air Situation Data Exchange, an eligible Potential ASDE Partner (PAP) Nation should submit a written request to participate in ASDE programme to the NATO Air and Missile Defence Committee. According to the NATO Policy on ASDE PO(2017)0452 the Vice Chairman is then responsible to staff the request for approval by the relevant Alliance bodies and the NAC. After approval, a Customer Request Form may be submitted following normal procedures.

Available on: The Application Layer Firewall for Link 1 (NATO Side) supports any security classification as required by the data handled reaching from NC to NS. The ALF-L1 (Partner Side) supports any security classification as required by the data handled reaching from NU to NC. The product software itself is classified as NR and the system is delivered as an NR system with software pre-installed.

Service prerequisites:

- PLT013 (former APP051) NATO Integrated Secure Platform – (NISP) Service
- Existing serial Link 1 connections must be available
- Communication lines, network infrastructure

Standard Service Support:

Support Hours:

Centralised Service Desk specialist agents are available during:

Monday to Thursday: 0600 to 2200 (CET)
Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

Belgium +32 65 44 3177
Netherlands +31 70 374 3177
Italy +39 081 721 3177
Germany +49 282 4978 3177
USA +1 757 747 3177
For NATO HQ +32 02 707 5858

Service Requests:

To request the APP052 service please complete the Customer Request Form and contact NCI Agency Demand Management. https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

To find the latest updates and most recent information about this service, please visit:

Internet: https://www.asc.nato.int (password protected – please request account at amdc2.productservices@ncia.nato.int)

NS WAN: https://airc2-iss.ncia.nato.int/support/

KPIs:
Due to the nature of the ASDE service (software running at system-high mode on unreachable and non-NATO networks) no service availability monitoring KPIs can be defined.
In terms of service support metrics, the standard Agency KPIs (per priority response times) apply for remote support. In case local intervention is required, the restoration time will depend on travel options at the time of the incident.

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

> **N.B.** Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: Unit of measure used for service quantification for each flavour is listed in the table below.

Service ID	Service Name	Service Flavour/Option	Service Unit
APP052	Situation Data Exchange (ASDE) Gateway	NCS-wide ALFL1 software maintenance and in service support	1

Service ID	Service Name	Service Flavour/Option	Service Unit
APP052	Situation Data Exchange (ASDE) Gateway	ASDE Gateway National Instance	Per instance

APP053 Multi Airborne Early Warning Ground Integration Segment Site Emulator (MASE) Application Service

Service ID: APP053

Service Name: Multi Airborne Early Warning Ground Integration Segment (AEGIS) Site Emulator (MASE) Application Service

Portfolio Group: Application Services

Service Description: The MASE Application Service provides a NCI Agency product and support of it, with the following purpose:

- Production of a real-time recognized air picture (RAP);
- Identification and exchange of the RAP with other military or civilian entities;
- Battlespace management and provision of weapons guidance solutions;
- Flight Plan processing and real-time interface to feeds supplied by ATC centres.

Value Proposition: MASE is a flexible, state-of-the-art solution to support the execution of air operations. Both military and civilian radars can be connected using a large variety of interface protocols on dedicated lines or packet switched networks. The sensor data from these sources is processed using a multi radar tracker, which produces the real-time air picture which can then be forwarded to other military installations. Flight plan data from civilian or military Air Traffic Control (ATC) centres are received, correlated with the real-time air picture and displayed to the operational user to support identification of aircraft. The Battlespace Management function assists the operational users in threat assessment and allocation of weapon resources. With the optional addition of the CRC System Interface (CSI), command and control can be performed on datalinks including Link 11(A&B) and Link 16. Threats can be engaged with either fighters or surface-to-air missile (SAM) units. When engaging with fighters, the assigned intercept controller can select between various types of guidance solutions depending on the fighters' capabilities and the prevailing tactical situation.

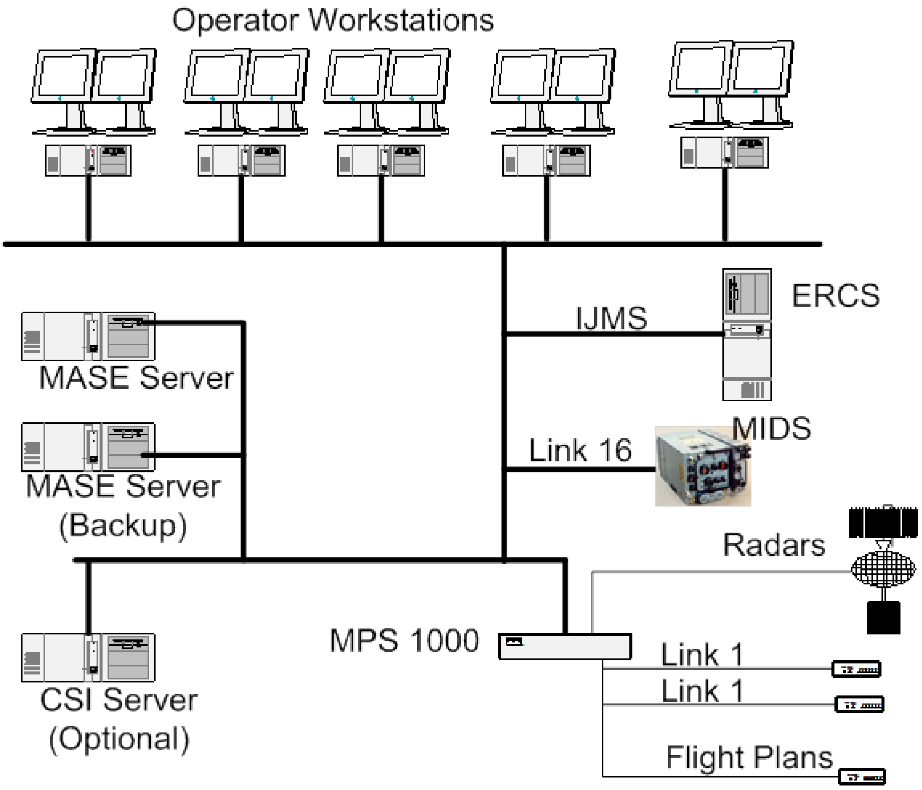
Service Features:

Sensor Integration – Allows to connect any number of radars to produce a locally generated Air Picture. Radar interfaces include but are not limited to : ASTERIX, JASR8, RMP, DDL, HADR, CD2, RSRP, T101, Cardion, T92, (A)S29, S743D, SRT, RAT31DL. The RAP produced is correlated into the Common Operating Picture (COP) and forwarded to connected units using the Link 1 interface.

Command and Control – Though the flight plan interface, tracks created from the RAP Production can automatically be identified. The Identification is managed with neighboring CRC's using the standard Link 1 messages for maintaining consistency across different military locations. The Weapons Allocator functionality allows for interceptor guidance and pairing to be performed. In addition, with the CRC System Interface (CSI) extension, Command and Control can be performed across the Link 11A/B and Link 16 datalinks. Enabling the operator to manage not only fighters but also land and naval units.

User Interface – The MASE User Interface has been completely re-designed, implemented upon a modern GUI engine and made more maintainable through the use of Java development. In the future, the legacy console will be completely replaced by the new MASE Integrated Console Environment (MICE). MICE has been developed together with the NPC CSI Section to ensure that future HMI updates can be achieved in a quicker, more cost effective manner.

Below figure outlines MASE in a typical use case:



Supported configuration – MASE encompasses client server architecture, with dedicated server applications for the main tasks as real-time air picture establishment and interfacing external systems, interconnecting dedicated MASE operator workstations for the operational display through a standard UDP/IP network. The serial interfaces (for both radars and flight plans) are brought into the MASE system through the MPS-1000 serial interface device.

Supported Interface Standards – JASR8, RMP, DDL, (A)S29, RAT31DL, HADR, ASTERIX, CD2, RSRP, S743D, T101, Cardion, T92, SRT. Through the CSI, the following interface standards are supported: Link 16 Link 11A, Link 11B, ATDL-1, Link 22, FFI, VMF, OTHT-Gold.

Supported data link interfaces – Link 1 in accordance with STANAG 5501, IJMS .

Hardware- Software and CIS requirements:

- NCI Agency (NPC) Integrated Solaris platform (NISP) as a secured Solaris OS platform;

- X86 or SPARC based server HW able to run NISP/Solaris;
- MPS-1000 Serial interface server;
- Communication lines, network infrastructure.

MASE is supported by:

- Provision of MASE Software
- Helpdesk and provision of level 1 to 3 support through the Helpdesk
- On-site interventions for installation and/or trouble shooting
- Engineering/application support covering:
  - Product and Configuration Management;
  - Product baseline updates;
  - Safety assessment supporting a customer side SIL 1 claim.

Service Prerequisites:

WPS001 – Managed Devices

PLT013 (former APP051) NATO Integrated Secure Platform (NISP) Service. The MASE server service flavour requires the NISP service as NISP is the recommended platform for MASE server on NATO networks. MASE clients can run on Windows environments and hence are not dependent upon PLT030.

Additional requirements:

- Existing serial Link 1 connections must be available
- Existing radar interfaces must be available
- If required, flight plan interfaces should also be available.

Service Flavours:

MASE software maintenance and in service support: (singleton service provided to SHAPE) Includes the development, testing, documentation and release of the MASE baseline to all sites registered for MASE. However, the sites themselves are responsible for the system update.

MASE instance installation and in service support: Upon request from non-NCS customers, MASE instances can be provided through an installation service. Such services and related support are requested through a Customer Request Form and implemented via a Technical Agreement to be funded by the service requester.

Available on: MASE supports any security classification from NC to NS.

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

- Monday to Thursday: 0600 to 2200 (CET)

- Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 CET).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

Belgium	+32 65 44 3177
Netherlands	+31 70 374 3177
Italy	+39 081 721 3177
Germany	+49 282 4978 3177
USA	+1 757 747 3177
For NATO HQ	+32 02 707 5858

Service Requests:

To request the APP053 service please complete the Customer Request Form and contact NCI Agency Demand Management. https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

The overall MASE availability target (99.5% yearly) is calculated as the combined availability of all of the following components (user identifiable functions):

MASE functional component	Target Availability	Performance threshold (initial access time)	Remarks
MASE Server Application (MSA)	≥ 99.5%	30”	Administrators should be able to load the MASE Server Application (AMA) within 30 sec.
MASE Console Application (MCA)	≥ 99.5%	20”	User should be able to access MASE Console Application (MCA) within 30 sec.

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Available NCI Academy Training not covered by service cost:

A1011	MASE - MICE CONSOLE MIGRATION (MMC)

Service Cost / Price: Unit of measure used for service quantification for each flavour is 1. Service Initiation and In-Service-Support will be provided and charged in accordance with the scope and financial estimates developed and agreed through site specific Technical Agreements.

Service ID	Service Name	Service Flavour/Option	Service Unit of Measure
APP053	MASE Application Service	MASE software maintenance and in service support	1
APP053	MASE Application Service	MASE instance installation and in service support	1

APP054 L16@29k Application Service

Service ID: APP054

Service Name: L16@29k Application Service

Portfolio Group: Application Service

Service Description: The Link 16@29K system allows a Host system to connect to a MIDS terminal and it:

- Allows the exchange of Link 16 (Platform D) data with other units on the same Link 16 network.
- Allows the MIDS terminal to be remotely controlled (On / Off Standby);
- Monitors the system discretes of the Link 16 Ground Equipment Suite.

Value Proposition: L16@29K allows the exchange of encrypted Link 16 data with other units on the same Link 16 RF Network. When connected through IP based crypto's the L16@29K allows for remote MIDS to be connected to a central C2 system

Service Features: L16@29K supports the following features:

- Local Mode : The L16@29K system is directly connected to the C2 host system using a MIDS Platform D interface. The MIDS is connected directly to an antenna at the physical location of the C2 host system.
- Remote Mode : The L16@29K system is situated in a remote location (due to UHF Coverage limitations). The system shares a platform D interface with the host system across an encrypted TCP IP connection. The MIDS is connected directly to an antenna at the remote location and is controlled remotely from the C2 host system.

Supported Interface Standards: The L16@29K system implements the Tactical Data Link protocol Link 16 in accordance with STANAG 5516, edition 2. The Platform D interface is currently supporting Block Cycle release 2. During 2021 the L16@29K Service will be updated to also include the Block Upgrade-2 (BU-2) interface for MIDS terminals.

Service Flavours:

L16@29K software maintenance and in service support: (singleton service provided to SHAPE) Includes the development, testing, documentation and release of the L16@29K baseline to all sites registered for L16@29K. However, the sites themselves are responsible for the system update.

L16@29K instance installation and in service support: Upon request, L16@29K instances can be provided to non-NCS customers through an installation and support service. Such services are requested through a Customer Request Form and implemented via a Technical Agreement to be funded by the service requester.

Available on:

NATO Secret

Service Prerequisites:

None

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

- Monday to Thursday: 0600 to 2200 (CET)
- Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 CET).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

Belgium +32 65 44 3177
Netherlands +31 70 374 3177
Italy +39 081 721 3177
Germany +49 282 4978 3177
USA +1 757 747 3177
For NATO HQ +32 02 707 5858

Service Requests:

To request the APP054 service please complete the Customer Request Form and contact NCI Agency Demand Management. https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

The overall L16@29K availability target (99.5% yearly) is calculated as the combined availability of all of the following components (user identifiable functions):

L16@29K functional component	Target Availability	Performance threshold (initial access time)	Remarks
L16@29K Application (LSA)	≥ 99.5%	10”	ACCS System capable of connecting to L16@29K Equipment Suite
MIDS Terminal Availability	≥ 99.5%	10”	MIDS Terminal capable of responding to interrogations from L16@29K Equipment Suite

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: Unit of measure used for service quantification for each flavour is 1. Service Initiation and In-Service-Support will be provided and charged in accordance with the scope and financial estimates developed and agreed through site specific Technical Agreements.

Service ID	Service Name	Service Flavour/Option	Service Unit of Measure
APP054	L16@29K Application Service	NCS-wide L16@29K software maintenance and in service support	1
APP054	L16@29K Application Service	L16@29K Instance installation and in service support	1

APP055 Core Geographic Information System (GIS) Application Service

Service ID: APP055

Service Name: Core Geographic Information System (GIS) Application Service

Portfolio Group: Application Services

Service Description: The Core Geographic Information System (GIS) Application Service is composed of subservices, which serve multiple purposes. The service is primarily based on the commercial off-the shelf ESRI software provides other Functional Services with a common set of geospatial information (Geospatial Service) to ensure that 'everyone is operating off the same map', thereby eliminating the need for other FSs to develop their own mapping solutions and maintaining their own set of geospatial information. In addition, the Core GIS enables anyone in the NATO Command Structure (NCS) to see available geospatial information like maps or imagery. Core GIS provides base maps/foundation Geospatial Information (GI)/geo location reference to all users and systems. The Core GIS also contains a functional area system (Geography Service) for dedicated geo professionals to enable the Core GIS Geospatial Services to be managed and administered. The Geography Services is implemented at each NCS site with high-end workstations and displays, large format plotting, and scanning infrastructure.

Value Proposition: The Core GIS Application Service provides customers with a suite of data, services and products that ensure all phases of military operations are conducted on the same spatial reference. Furthermore, it provides the Accredited/Single Geospatial Information Service Provision (authoritative repository for Geospatial Information).

Service Features: The current Core GIS Application Service consists of:

> **Cartographic Workshop**, which allows Geo-Technicians to create and maintain the Digital Geographic Information baselines, generate products, and publish and maintain geospatial services via the NATO Core GIS Server. The Cartographic Workshop comprises several high-end workstations for geo processing, and other peripherals such as an A0 plotter, A0 scanner, office printer, DVD production station, and infrastructure equipment
>
> **The Core GIS Server**, which is used to provide geographic products such as electronic maps or other geospatial information in digital form to Functional Services and FASs using international standards such as Web Map Service (WMS), Web Feature Service (WFS), Web Coverage Service (WCS), Web Processing Services (WP).

Service Flavours: The service is available as a single flavour.

Available on: NATO Bi-SC Core GIS service is available on the NS, MS, KFOR and RSM network. However, the service may be available on the customer's choice of security domain, as well. In case of national security domain, the customer is responsible for the accreditation and license module.

Service Prerequisites:

WPS001 Managed device service.
Client: Windows 7 or Higher
Server: Windows 2012 R2 or Higher.
Detailed HW/SW requirements available upon request

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A0300	Geo Basics Level 1
A0301	Geo Basics Level 2
A0302	Geo Scenario
A0310	Core GIS Servers
A9042	Combined Situational Awareness Functional Area Services for CTE/exercise

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP056 ISR Collection Management Tool (ICMT) Application Service

Service ID: APP056

Service Name: ISR Collection Management Tool (ICMT)

Portfolio Group: Application Services

Service Description: The ICMT Service provides a capability to effectively manage the satisfaction of Prioritized Intelligence Requirements (PIRs): plan, task, monitor theatre-wide ISR collection capabilities, manage intelligence documents, and disseminate products. It also facilitates the collection of short-notice requests and requirements in a timely manner. The ICMT Tool has two functions: Intelligence Requirements Management function (IRM) and Collection Management function (CM), of which IRM usually is not used by the NATO entities. Collection Management function supports users in developing and disseminating CRs. The purpose of CRs is to combine (or bundle) similar Essential Elements of Information (EEIs) from the ICP (similar with regards to locations, time and required ISR capabilities) to propose doing as much as possible with the limited ISR resources. CRs are recorded and tracked in the ISR Plan with associations to the EEIs that they satisfy in the ICP. The system provides support to process Collection Requirements List (CRL) and Collection Task List (CTL). When collection coordination is required CRs are passed up the chain of command as validated and prioritised CRs in the CRL. At the joint level CRs assigned to subordinate commands/units are disseminated as CTL. ICMT provides support to develop and disseminate Collection & Exploitation Plan (CXP). The CXP is the plan that provides detail of the tasks assigned to specific ISR capabilities to meet the formation's collection requirements. The CXP is based upon own formation's or CRs assigned from the JCMB received through the CTL. ICMT also provides functionality to disseminate CRs as ISR Requests and Tasks (ISRRs), and to manage received ISRRs.

Value Proposition: ICMT is a client/server solution making it possible for the different roles involved in the IRM & CM processes to work in parallel on a common database. Support for development of Intelligence Requirements and Intelligence Collection Plan (ICP) is provided in the new Intel Collection Plan workspace. Support for the management of Requests for Information (RFI) is improved and now supported in the new Requests workspace. Additional values are:

- Support for dissemination of the ICP in xml format.
- Support for development of both Collection Requirements (CR) and ISR Plans are new capabilities provided in the ISR Plan workspace.
- New capabilities to manage ISR Requests (ISRREQ) and ISR Tasks, which is a significant improvement of support for Collection Management. Collection Requirements can easily be exchanged between commands and ISR units as ISR Requests and ISR Tasks.
- Dissemination of the Collection Task List (CTL) in xml format is supported.
- Support to import of and export to excel sheets that comply with MAJIIC 2 Bravo .1 Baseline for the information content.

- Configurable to connect to the MAJIIC 2 Bravo .1 JISR COI Technical Services enabling interoperability with national and NATO systems that are Bravo.1 compliant.

Service Features:

- Intelligence Requirement Management
  - Develop, receive, manage and track Priority Intelligence Requirements (PIRs) and IRs.
  - Developing and maintaining the ICP.
- Collection Management
  - Develop and disseminate CRs (CRLs and CTLs)
  - Process Collection Requirements List (CRL)
  - Process Collection Task List (CTL)
  - Develop and disseminate Collection & Exploitation Plan (CXP)
  - Functionality to disseminate CRs as ISR Requests and ISR Tasks (ISRRs)
  - Manage received ISRRs.

Service Flavours: The service is available as a single flavour.

Available on:

NATO Secret

Service Prerequisites:

WPS001 Managed Device Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A9030	Intelligence Collection Management Tool (ICMT)

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP057 INTEL FS SIGINT Capability (ISC) Application Service

The Service is classified. Further information is available upon request and relevant clearance.

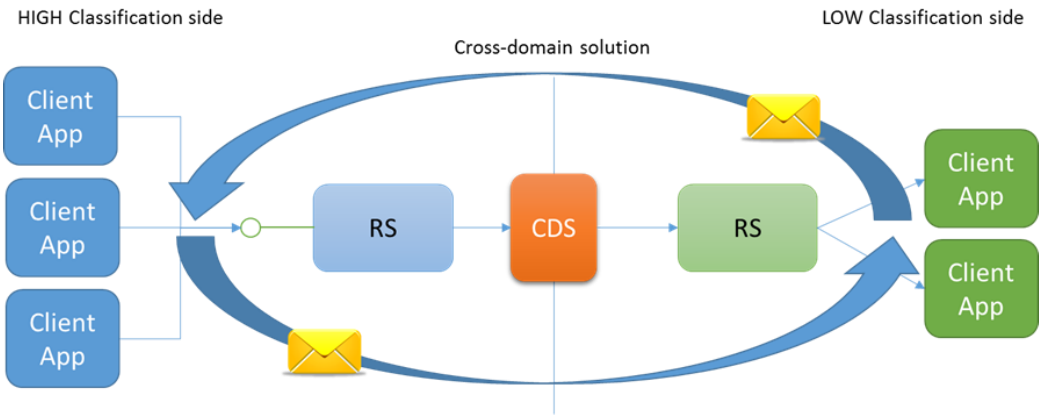
APP058 Release Server (RS) Application Service

Service ID: APP058

Service Name: Release Server (RS) Application Service

Portfolio Group: Application Services

Service Description: The Release Server (RS) service interface provides an abstraction layer for applications to release information between two security domains of different security levels. The service hides the complexity of Cross Domain Solutions for client applications.



Value proposition: The RS provides a service interface for applications to release information between two security domains of different security levels. The complexity of cross domain solutions are hidden behind a simple service interface. The Release Server supports automated and controlled release of information (a man in the loop scenario).

Service Features:

The Application features:

- Configurable release rules based on release-ability markings (Authority, Classification and Release-ability);
- Automated or controlled (man in the loop) release of information;
- Monitoring;
- Fully Web based user interface;
- Fully documented;
- Automated installation package.

Support features:

- * Support to implementation, integration and customization;
- * Support to operations and maintenance;
- * Support to training requirements;
- * Information gathering for technical and training support.

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Secret
Mission Secret

Service Prerequisites:

Hardware:

- 64-bit architecture processor (multiple cores).
- Minimum 4 GB RAM (recommended 8 or 16 GB for operational use).
- 100 GB System drive.
- 500 GB Data drive minimum (depending on usage).

Software:

- MS Windows 2012 or newer
- IIS
- .NET Framework 4.6.2
- MS SQL Server 2008R2 or newer

The service can be configured remotely using a HTML5 compatible browser.

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP059 Joint Exercise Development and Management (JEMM) Application Service

Service ID: APP059

Service Name: Joint Exercise and Management (JEMM) Application Service

Portfolio Group: Application Services

Service Description: The Joint Exercise Development and Management Application Service supports exercise training audiences in developing training objectives in a phased manner using a set of reference training objectives. JEMM subsequently supports exercise scenario designers in developing the MEL/MIL (Master Event List/Master Incident List) for an exercise in a structured and deliberate manner according to the process specified in the Bi-SC Directive 75-3. The application service also supports an exercise control organisation in executing the MEL/MIL during an exercise in a collaborative, distributed and interoperable manner. The exercise observation and analysis process is also supported. A specific flavour of JEMM supports the BMD community in executing BMD exercises by providing a direct interface to the BMD version of APP069 ITC.

Value Proposition: This application service supports exercise training audiences, exercise scenario managers, control staff, observers and analysts in performing their tasks in the preparation and execution of an exercise in a distributed and collaborative manner. It adds value to the process of developing, executing, observing and analysing an exercise by:

- Providing support for maintaining an organisational level of reference Main Capability Areas and subordinated tasks
- Providing support for a simple and advanced mode for developing training objectives. The advanced mode provides a controlled workflow for training audiences and training organisations to develop training objective descriptions to manage exercise resourcing conditions and achievability status and to set their priorities.
- Providing support for a collaborative and distributed way of working during the preparation and the execution of an exercise MEL/MIL.
- Providing a structured way of describing the MEL/MIL according to the Bi-SC 75-3.
- Establishing an explicit relationship between training objectives and MEL/MIL.
- Establishing explicit relationships between training objectives, observations and analysis
- Implementing a tailored workflow for the development and execution of a MEL/MIL.
- Implementing a tailored set of states for observations and analysis that are linked to training objectives.
- Providing, in a single configurable view, the elements of exercise information that are critical to the implementation of specific roles in the exercise control organisation.
- Providing the ability to add new sources of exercise information without having to modify the exercise control business applications.

- Documented capability to rapidly build exercise control dashboards using regular office automation tools.
- Providing the ability to configure and manage the execution of automated real time or periodic reporting data feeds capable of depicting ground, air, maritime, logistic and intelligence pictures.

Service Features: The JEMM Application Service supports the distributed, collaborative and structured development, execution, observation and analysis of an exercise MEL/MIL. Specifically, JEMM offers the following features:

- Prepare and develop the MEL/MIL as specified in the Bi-SC 75-3 Directive.
- Prepare and describe the synchronisation with simulation-based or live support to the exercise.
- Manage the execution of the MEL/MIL
- Manage the synchronisation of activities with simulation-based or live support to the exercise.
- Prepare and manage the collection of observations by observer/trainers.
- Analyse the collected observations and assess the progress of training objective achievement.
- Assign roles and rights to various users to perform tasks relevant to their participation in the exercise.
- Tailor the workflow of the execution and observation processes.
- Document MEL/MIL, observations and analysis results.

In addition the JEMM Application Service provides a structured, documented distributed access to configure data access to other NATO-operated exercise services like JTLS, JCATS and VBS as well as the ability to user-provided data in Excel spreadsheets. Access to specific JOCWATCH incident data is also supported. In order to visualize and exploit the combined data in an effective manner, JEMM offers a number of features that enables an exercise control organisation:

- To compose and visualize an exercise common operational picture in a distributed and collaborative manner.
- To de-conflict MEL/MIL with training audience activities and battle rhythm meetings
- To gather and extend MEL/MIL dashboards.

The JEMM Application Service also includes the feature to generate a subset of AdAt-P3, and OTH-GOLD messages as well as tactical links according to Link 16 and NFFI standards from data provided by the NATO-operated exercise services JTLS, JCATS and VBS.

In a specific BMD mode, the JEMM application service can be configured to communicate with the ITC (BMD) simulation service provided by APP069. Through JEMM, ITC simulation actions can be executed at scheduled times and the simulation state can be returned and processed by the automated reporting features to deliver an effective near-real time BMD recognized picture.

Service Flavours: The service is available as two flavours. A non-BMD and a BMD flavour.

Available on:

NATO Secret
Mission Secret
PAN

Service Prerequisites:

WPS001 Managed Devices Service

Standard Service Support Levels:

Service Availability Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A5002	MEL/MIL
A5004	JEMM Data Administrator
A5006	Joint Exercise Management Module (JEMM) system administrator

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP060 ISR Coalition Shared Data (CSD) Service

Service ID: APP060

Service Name: ISR Coalition Shared Data (CSD) Services

Portfolio Group: Application Services

Service Description: The Service supports a wide range of CSD-dependent customer facing applications (CSD clients), including Exploitation and IRM&CM applications, and Sensor Systems. Currently, supported applications are HMART, ICMT, and INTEL-FS, as well as national applications. The Service:

- enables the exchange of NATO Intelligence, Surveillance and Reconnaissance (ISR) products through provision of a standard interface for storing, discovering, accessing and sharing heterogeneous ISR libraries maintained by NATO and Nations;
- provides workflow support to the overall JISR Process of Tasking, Collection, Processing, Exploitation and Dissemination (TCPED) spanning multiple echelons, multiple military services and multiple NATO and national applications and services; and
- provides access to live or recorded Streaming Data types, such as Full Motion Video, Video Clips, or Ground Moving Target Indicator (GMTI) data

Value Proposition: The Service supports the JISR systems, workflows, and processes in order to provide the right (intelligence) information, at the right time, in the right format and to the right location for commanders to make the right decisions.

Service Features: Intelligence Surveillance Reconnaissance Coalition Applications features in the following categories:

- CSD ISR Product Library: storage, discovery, access and dissemination
- CSD ISR Workflow: support for JISR Collection Management and TCPED Process
- CSD ISR Streaming: access to live or recorded streaming data types

Supported JISR data formats, interfaces, and technical service contracts: STANAG 4545, STANAG 4609, STANAG 4607, STANAG 5516, STANAG 4559, and MAJIIC2 Bravo .1 Baseline.

Service Flavours: The Service is available in multiple flavours, depending on the combination of the following independent component services:

- ISR Product Library Services
- ISR Workflow Services
- ISR Streaming Services

Available on:

NATO Secret
Mission Secret

Service Prerequisites:

WPS001 Managed device service

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP061 Air Command and Control Information Services (AirC2IS)

Service ID: APP061

Service Name: Air Command and Control Information Service (AirC2IS)

Portfolio Group: Application Services

Service Description: The Air Command and Control Information Service (AirC2IS) is the Air Functional Service including Ballistic Missile Defence(BMD of the Bi-Strategic Command Automated Information System (Bi-SC AIS) for all levels of the NATO Command Structure. It is a non-real-time Command and Control service, which provides the NATO air staff with an integrated, robust, flexible and automated capability to effectively plan, execute, monitor and assess Air Operations (including BMD operations) in a responsive and timely manner. Together AirC2IS and the Air Command and Control System (ACCS) provide NATO's complete Air C2 capability. AirC2IS is an integrated suite of applications that addresses the Air Command & Control (AirC2) requirements at the operational and strategic level, as specified in the Allied Joint Publication (AJP) 3.3(A). AirC2IS supports the NATO AirC2 cycle.

Value proposition: AirC2IS evolves with the collaboration of the operational community for the operational community to provide an integrated, robust, flexible and automated capability to effectively plan, execute, monitor and assess Air Operations in a timely manner. It is designed with a focus on collaboration and multi-system integration. It ideally supports the operational level planning, assessment and information knowledge management processes. It is especially suited to the joint environment at static or deployed locations.

Service Features: AirC2IS acts as an information hub between the air mission area and other mission areas (land, maritime, special operations forces, intelligence, logistics, and others). To be able to do this, AirC2IS consumes information from and provides services to several NATO systems, including ICC, NIRIS, LOGFAS, and NCOP.

Following functionalities are included in AirC2IS:

Mission Applications:

- Interactive Map
- C2OA Manager
- ORBAT Applications
  - Generic Catalogue
  - Own ORBAT Manager
  - OPFOR ORBAT Manager
  - Neutral ORBAT Manager
- TBMD Applications
  - OPFOR TBM COA Manager
  - PCAL Manager
  - JPCAL Manager
  - IDDM
  - SAWREP Manager

- Tactical Information Display
- CONOPS Manager
- Support to Air Logistics
- AOD Editor

Information Portal:

- HQ Portal
- Mission Portal

Service Flavours:

NCS-wide AirC2IS software maintenance and in service support: (singleton service provided to SHAPE) Includes the development, testing, documentation and deployment of maintenance releases of all AirC2IS software components and the continuous support of the eligible AirC2IS sites throughout the NATO Command Structure (NCS).
AirC2IS server: Provides an AirC2IS instance hosted on server infrastructure provided by the INF004 service, including local prerequisite COTS software, configuration, version updates and continuous support.
AirC2IS client: Provides support for an AirC2IS user on WPS001 Managed Devices to connect via web browser to an AirC2IS Server service instance.

Available on:

NATO Secret
Availability on any other NATO or national security domains is TBC upon a new service request.

Service prerequisites:

WPS001 – Managed Devices. AirC2IS clients require this service, which provides a standard NATO workstation connected to the NATO networks on which the AirC2IS web client application can be accessed.

INF004 - Infrastructure Virtualization Services to provide the server instances (either physical or virtual) on which the AirC2IS Server components can be deployed.

Standard Service support levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

Monday to Thursday: 0600 to 2200 (CET)
Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 CET).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

Belgium	+32 65 44 3177
Netherlands	+31 70 374 3177
Italy	+39 081 721 3177
Germany	+49 282 4978 3177
USA	+1 757 747 3177
For NATO HQ	+32 02 707 5858

Service Requests:

To request the APP061 service please complete the Customer Request Form and contact NCI Agency Demand Management.
https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

The overall AirC2IS availability target (99.5% yearly) is calculated as the combined availability of all of the following components (user identifiable functions):

AirC2IS functional component	Target Availability	Performance threshold (initial access time)	Remarks
AirC2IS Mission Application (AMA)	≥ 99.5%	30”	User should be able to access AirC2IS Mission Application (AMA) within 30 sec.
AirC2IS SharePoint Information Portal (AIP)	≥ 99.5%	20”	User should be able to access AirC2IS within 20 sec.
AirC2IS System Management Application (SMA) Access	≥ 99.5%	20”	FAS Managers, Data Managers, and System Administrators should be able to access the SMA within 20 Sec.
AirC2IS Legacy System Adapter (LSA) Availability	≥ 99.5%	N/A	LSA is AirC2IS backend interfaces component not visible to the user.

Defence Design Save Time	≥ 99.5%	30”	AirC2IS users should be able to save the AirC2IS Defence Design of up to 1000 data elements within 30 Sec.

KPIs implementation:

AirC2IS contains internal monitoring functionality. The necessary changes to expose the above availability KPIs are planned for implementation as part of the product roadmap.

Service Restoration:

Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Available NCI Academy Training not covered by service cost:

A1013	AirC2IS User
A1014	AirC2IS System Administrator
A1025	Situational Awareness with AirC2IS
A1026	Portal and Data Management of AirC2IS
A1027	BMD Planning with AirC2IS

Service Cost / Price: Unit of measure used for service quantification for each flavour can be found in the table below:

Service ID	Service Name	Service Flavour/Option	Service Unit
APP061	AirC2IS Application Service	NCS-wide AirC2IS software maintenance and in service support	1
APP061	AirC2IS Application Service	AirC2IS client	Per user

Service ID	Service Name	Service Flavour/Option	Service Unit
APP061	AirC2IS Application Service	AirC2IS server	Per instance (standard high availability AirC2IS server cluster)

APP065 Joint Tactical Simulation (JCATS) Application Service

Service ID: APP065

Service Name: Joint Tactical Simulation (JCATS) Application Service

Portfolio Group: Application Services

Service Description: The Joint Tactical Simulation Application Service supports exercise control organisations in maintaining a virtual situation of the battle space consistent in time and space in accordance with the decisions taken by the training audience and with the activities of other relevant actors in the synthetic world at a tactical level of decision-making. The tool used for the Joint Tactical Simulation service provides the Joint Conflict and Tactical Simulation (JCATS) system which is a US Government-Off-The-Shelf simulation application with a tailor-made interface application that supports the distributed and collaborative execution of training audience orders and exercise control guidance in a synthetic world. JCATS maintains the status of the synthetic environment and all represented joint forces in time and space.

Value Proposition: This application service supports exercise designers and control organisation in gathering and in managing all the detailed synthetic data that is required to realistically produce information flows towards the training and its supporting command and control applications in a manner that is consistent in time and space based on the activities and capabilities of deployed forces. The application service allows the many contributors to the preparation and execution of a computer assisted exercise (CAX) to perform their tasks in a distributed and collaborative manner. It adds value to the CAX preparation and execution process by:

- Providing support for a collaborative and distributed way of collecting all relevant ORBAT data in an efficient manner.
- Providing support for tactical levels of information to meet the requirements of the exercise training audience.
- Providing a very broad set of automated behaviours that allow the state of the synthetic world to be maintained in an automated manner.
- Providing the ability to capture execution data and re-using it for after-action-review processes.

Service Features: The Joint Tactical Simulation Application Service offers the following features:

- Capture and manage detailed information about entities that are relevant to the conduct and context of NATO joint major and small operations at various levels of intensity in a crisis response or collective defence context.
- Manage the behaviour of entities in time and space that are relevant to the conduct and context of NATO joint major and small operations at various levels of intensity including intelligence, logistics and combat aspects.

- Provides support to produce detailed information output about entities that are relevant to the conduct and context of NATO major and small operations at various levels of intensity in a crisis response or collective defence context.

In addition, the agency maintains a JCATS ORBAT Builder (JOB) application that supports exercise planners in building that part of the ORBAT for which they are responsible in a stand-alone manner in a format that is compatible with JCATS. An exported ORBAT file can be consolidated into a central JCATS exercise dataset by the exercise database developers.

Service Flavours: The Service is available as a single flavour.

Available on:

Mission Secret

Service Prerequisites:

WPS001 Managed Devices Service

Standard Service Support Levels:

Service Availability Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP066 Joint Operational Simulation Application Service

Service ID: APP066

Service Name: Joint Operational Simulation Application Service

Portfolio Group: Application Services

Service Description: The Joint Operational Simulation Application Service supports an exercise control organisation in maintaining a virtual situation of the battle space consistent in time and space in accordance with the decisions taken by the training audience and with the activities of other relevant actors in the synthetic world at an operational level of decision-making.

The Commercial-Off-The-Shelf simulation application adopted for this purpose is a sub-set of the modules provided by the Joint Theater Level Simulation (JTLS)[1]. The service features a distributed and collaborative preparation of scenario data, execution of training audience orders and exercise control guidance in a synthetic world and the capture of after-action-review data. JTLS maintains the status of the synthetic environment and all represented joint forces in time and space in an internal structure as well as in an externally accessible format.

Value Proposition: The Joint Operational Simulation Application Service supports exercise designers and control organisations in gathering and in managing all the detailed synthetic data that is required to realistically portray joint operations at an operational level across the spectrum of military operations. The application service allows the many contributors to the preparation and execution of a computer assisted exercise (CAX) to perform their tasks in a distributed and collaborative manner. It adds value to the CAX preparation and execution process by:

- Providing support for a collaborative and distributed way of collecting all relevant ORBAT data in an efficient manner.
- Providing support for the controlled simulation of joint operations at an operational level of detail across the spectrum of military operations.
- Providing a very broad set of automated behaviours that allow the state of the synthetic world to be maintained in an automated manner.
- Providing the ability to capture execution data and re-using it for after-action-review processes.

Service Features: The Joint Operational Simulation Application Service offers the following features:

- Capture and manage aggregated information about entities that are relevant to the conduct and context of NATO joint major and small operations at various levels of intensity in a crisis response or collective defence context.
- Manage the behaviour of entities in time and space that are relevant to the conduct and context of NATO joint major and small operations at various levels of intensity including intelligence, logistics and combat aspects.

- Provides support to produce aggregated information output about entities that are relevant to the conduct and context of NATO major and small operations at various levels of intensity in a crisis response or collective defence context.
- Providing access to its state information to external data consumers.

Service Flavours:

APP066-1 Joint Operational Simulation Application Service Centralised Capability

APP066-2 JTLS Approved Additional Modules service (JTLS_AAM)

This flavour provides an additional set of commercial modules that complement the Joint Operational Simulation Application Service Centralised Capability Model. This flavour ensures that the modules that are compatible with the operational APP066 application service are tested to be fit-for-purpose and are tested for cyber hygiene in the NATO enterprise.

The following JTLS-compatible additional modules can be made available in combination with APP066:

- JTOI (*jtoi_icc340*)
- JOI_L16 (*l16ms*)
- JOI_OTHG (*othgms*)
- JOI_LC2IS (*lc2ms*)
- JLOI (*logfasts*)
- MDP (*mdp*)
- ATOP (*icc_68atop*) – ATO Parser
- ATOT (*atot*) – ATO Translator
- AARC (*aarc*)
- SDC (*sdc*)
- DDS Glassfish (*started with script: dcp*)
- OVT Order Verification Tools (*started with script: jovt*)

Available on:

For APP066-1 Joint Operational Simulation Application Service Centralised Capability is available on Mission Secret[1]

For APP066-2 JTLS Approved Additional Modules service (JTLS_AAM) is available on M166 and NS in Stavanger.

Service Prerequisites:

WPS001 Managed Devices Service

Standard Service Support Levels:

Service Availability Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

[1] The included JTLS modules are: DDS, SIP, ICP, CEP, JODA, JXSR, OMA, XMS, SYNAPSE, WHIP, SDC, OEC, AARC, OVT, ATO-T

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP067 RECCEN Application Service

Service ID: APP067

Service Name: Record Centre (RECCEN)

Portfolio Group: Application Services

Service Description: The Service provides the collaborative information management capability for Records Management, with functionalities for record keyword tagging, storage, search and retrieval. The highest content classification of records stored is limited by the security accreditation of the respective network the service is deployed on.

Value proposition: The Service offers the customers the benefit to easily access and maintain records information by providing information access control, locating and retrieval of records.

Service Features:

The Service offers the user:

- Upload of documents
- Document validation by the Registry as a “Record”
- Meta tagging of the records
- Records classification enforcement
- Records categorization
- Access control
- Browsing of records
- Search, discovery and retrieval of records
- Providing permanent links to records.

Service Flavours: The service is available as a single flavour.

Available on:

	PUBLIC	UNCLASSIFIED	RESTRICTED	SECRET	MISSION SECRET
REACH			X*		
Bi-SC AIS				X*	
Federated Access (NR)			X**		
Federated Access (NS)				X**	

Service prerequisites:

* WPS002 Enterprise Identity Access Management Service
** PLT005 Active Directory and Federation Service
WPS003 Enterprise User License Service (or any other valid SharePoint Client Access License (CAL))
PLT003 Web Hosting Service

Standard Service support levels:

Service Availability Target: 99%

Service Restoration Priority: P3.

The Standard Service support comprises the following activities:

- **Operation**: application monitoring, log management, batch jobs management, backup & restore, auditing, Service Requests fulfilment.
- **Corrective Maintenance**: diagnosis and removal of the causes and the effects of any malfunction affecting the Service.
- **Preventive Maintenance**: preventive actions needed to avoid future malfunctions
- **Adaptive Maintenance**: adjustment of the Service in order to adapt to the minor changes of the sub system components (i.e. Operating System, Database Management System, Browser, SharePoint and SharePoint add-ons). Major changes of the sub system components shall be requested via dedicated projects.

Service Cost / Price:

The unit of measure for the Service is "per user". Since the Service is designed for the general use by all the users of each customer, the number of user will be based on the principal numbers equivalent to the sum of the "NATO Peacetime Establishment (PE)" users plus the "NATO Non-Peacetime Establishment (NPE)" users as per SOR/MER 2023.

For customers not listed in the SOR/MER 2023, the number of users will be based on the agreed number of prerequisite WPS002 or PLT005 units in relevant SLA/SSP.

The cost of the Service does not include the cost of all the underlying Service prerequisites.

APP068 Advisor Network (ANET) Application Service

Service ID: APP068

Service Name: Advisor Network (ANET) Application Service

Portfolio Group: Application Services

Service Description: The Advisor Network (ANET) Application Service provides services for planning, coordinating, reporting, analyzing and archiving partner engagements. Originally designed to support Advisors engaging partner nations in the scope of Train Advise and Assist missions, it has been since also enhanced to a broader context of stakeholder engagement managements. It provides an audit trail of past engagements and people, as well as the ability to assess additional elements such as partner capabilities, engagement coverages and mission objectives. It provides capabilities commonly found in Customer Relationship Management (CRM) tools, while strongly tailored to support NATO-specific requirements.

Value proposition: The ANET Application Service is an online tool (web-based) to support users when planning, coordination and reporting partner engagements. Over time, an audit trail of past engagements and partners is build up in ANET's database. ANET's advanced search and visualisation capabilities make it easy for advising organizations and mission leadership to gain context on engagements which can shape future decision making.

Service Features: ANET is a web-based tool with the following features:

- Record, collate and store engagements
- Plan and coordinate future engagements
- Gain and maintain partner relationships on both organisational and personal levels
- Assess partner personal and organizational capabilities, mission objectives and progress
- Understand and improve engagement coverage
- Advanced search, analytics and visualisation capability including GIS

Service Flavours: The Service is available in 3 flavours, based on the number of users:

- Small deployment: 0-200 users
- Medium deployment: 200-2,000 users
- Large deployment: 2,000-10,000 users

Available on:

Internet
NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

Service prerequisites:

WPS001 - Managed Device Services – for application instances installed on NCI Agency managed networks.

Standard Service support levels:

Service Availability Target: 99.5%

Service Restoration: Where the service is deemed unavailable, depending the SLA for the hosted environment, the service restoration period for a critical incident (i.e.1 P0/P1) will be between 4 hours and 72 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the service is Per Deployment. Price details available in the Service Rates Document.

APP069 Air Integrated Training Capability (ITC) Application Service

Service ID: APP069

Service Name: Air Integrated Training Capability (ITC) Application Service

Portfolio Group: Application Services

Service Description: The Air Integrated Training Capability (ITC) Application Service supports air commands exercise control organisations in maintaining a virtual situation of the battle space consistent in time and space in accordance with the decisions taken by the training audience and with the activities of other relevant actors in the synthetic world. In addition the service supports the exercise control organisation in generating relevant and compatible information flows to the training audience automated air command and control systems and in extracting structured order information from those systems. ITC provides a separate version that has been extended with specific models and behaviours for Ballistic Missile Defence (BMD) sensors, weapon systems and threats. ITC (BMD) interacts with the APP059 Joint Exercise Management Module (JEMM) for scenario preparation, execution and interoperability.

Value Proposition: The ITC application service supports exercise designers and control organisation in the air C2 community in gathering and in managing all the detailed synthetic data that is required to realistically produce information flows towards the training audience and its supporting Air C2 systems. The application service allows the many contributors to the preparation and execution of an Air C2 computer assisted exercise (CAX) to perform their tasks in a distributed and collaborative manner. It adds value to the CAX preparation and execution process by:

- Providing support for a collaborative and distributed way of collecting all relevant ORBAT data in an efficient manner using a familiar interface.
- Providing interoperability with NATO Air command and control systems in an efficient and flexible manner.
- Providing a very broad set of automated behaviours that allow the state of the synthetic world to be maintained in an automated manner.
- ITC (BMD) integrates with JEMM to provide the simulation of BMD scenarios either as a stand-alone capability or in combination with other simulations through the DIS protocol.

Service Features: The ITC system is built upon a Commercial-Off-The-Shelf simulation framework (FLAMES). ITC provides an air exercise control organisation with the ability to simulate air operations as defined in an Airspace Coordination (ACO) and Air Tasking Order (ATO) for two opposing and one neutral side. An exercise controller can manage the overall execution of the scenario and influence the adjudication of simulation outcomes. The resulting status updates are fed automatically into the Integrated Command and Control (ICC) in the form of air tracks, status updates and messages. ITC (BMD) integrates with JEMM to provide the simulation of BMD scenarios and produce shared early warning and Link-16 tactical data links either as a stand-alone capability or in combination with other simulations through the DIS protocol.

Service Flavours: The Service is available as a single flavour.

Available on:

Mission Secret

NATO Secret

Service Prerequisites:

WPS001 Managed Devices Service

APP059 Joint Exercise and Management (JEMM) Application Service for ITC (BMD)

Standard Service Support Levels: The NCI Agency offers service support packages for AirC2 applications and systems defined by the provided service levels and set of support tasks. The support tasks can be all or a subset of the following group of tasks:

XAA	First Line Support
XAB	Second Line Support
XGM	Third Line Support
XAD	Data and Document Provisioning
XDC	Contract and License management
XBC	Installation
XCC	Interoperability Management
XDD	Product Maintenance
XGC	Security
XGJ	Obsolescence management
XBB	On-site maintenance
XBD	Site Support
XFA	Individual Technical training
XGK	Technical Manuals
XED	ILS management
XGI	Deployment of deployable equipment
XCB	System status and statistics
XGF	Database management and engineering
XFB	Support to OT&E and exercises
XIC	Platform and tools support

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Available NCI Academy Training not covered by service cost:

A1015	Integrated Training Capability (ITC) Technical Control Officer (TCO)

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP070 Training Objective Development and Management (TOMM) Application Service

Service ID: APP070

Service Name: Training Objective Development and Management (TOMM) Application Service

Portfolio Group: Application Services

Service Description: The Training Objective Development and Management Application Service supports exercise training audiences and associated training organisations in producing a structured and prioritised set of training objectives for a particular training event and phase in a collaborative and distributed manner according to the process in the Bi-SC Directive 75-3. An organisational set of reference training objectives can be maintained and used as the basis for the development of exercise-specific training objectives.

In addition, the application service supports exercise training audiences and associated training organisations in managing training objective resource conditions in a distributed and collaborative management according to the guidance described in the Bi-SC Directive 75-3 throughout the exercise preparation phase.

Value Proposition: This application service supports exercise training objective owners and supporting resource condition owners in developing training objectives according to the Bi-SC Directive 75-3 in a structured manner. It adds value to the process of developing and managing training objectives by:

- Providing the ability to manage a set of reference training objectives
- Providing support for a collaborative and distributed way of working.
- Providing support for the workflow between the stages of development.
- Providing an explicit statement of resource requirement and acknowledgment by resource owner.
- Providing a real time up to date dashboard of the state of achievability of training objectives throughout the exercise planning and preparation process
- Reducing travel and coordination effort.
- Enabling a wider participation in the process by training audience personnel and resource owners.

Service Features: The features of the Training Objective Management Module (TOMM) are:

- Act as an organisation training objective manager to create, update and delete reference training objectives including resourcing conditions.
- Act as a Training Objective Manager capable of managing the contributions and workflow of the TO development process including the prioritisation
- Act as Training Objective Scripter capable of defining the content of training objectives, the associated resourcing conditions and standards
- Act as a resourcing condition owner capable of commenting and acknowledging resource requirements.

- Develop training objectives according to the stages and format specified in the Bi-SC Directive 75-3 ..
- Review training objectives and associated resource conditions in a collaborative and distributed manner
- Manage and track the achievability state of the training objective resourcing conditions.
- Prioritise training objectives and re-organise their sequence accordingly.
- Review and update the achievability of resource conditions in a dashboard until the start of the exercise.
- The TOMM training objectives are fully compatible with the training objectives of APP059 JEMM.

Service Flavours: The Service is available as a single flavour.

Available on:

Mission Secret
NATO Secret

Service Prerequisites:

WPS001 Managed Devices Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Available NCI Academy Training not covered by service cost:

A5003	Training Objective Management Module (TOMM)

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP071 Enterprise Business Application (EBA) Service

Service ID: APP071

Service Name: Enterprise Business Application (EBA) Service

Portfolio Group: Application Service

Service Description: The EBA service is built as an integrated system of systems tailored to support a number of enabling processes for day-to-day operational activities of the NATO C&I Agency processes. The service can be offered as-is as an extension of the operational service defined for the NATO C&I Agency through the execution of a project. Alternatively, the service can be replicated and adapted to meet specific customers' needs subject to proper analysis and implementation though a fully funded project.

Value Proposition: The Service is designed and implemented to support a defined set of processes currently in place at NATO military and civilian organisations. It meets the requirements defined for customer funding regime and the relevant NATO committees. It is operational and used by NCI Agency and can be extended, deployed and adapted to any NATO body or national entity.

Service Features: The Service provides support to:

- All financial processes in line with IPSAS;
- Full acquisition processes including the direct interaction with the industry for ordering services and supplies;
- NATO specific Travel process;
- Most of the HR processes;
- Management of assets (ICT and non-ICT);
- Full P3SM process to manage Portfolio, Programs, Projects, Services and Resources;
- Reporting for each function/process area;
- Enterprise Reporting (Business Intelligence) across functional/process areas.

Service Flavours: The Service can be tailored to include only specifically required features to meet specific customer needs.

Available on: The service is available on NU with some elements on NR.

Service Prerequisites: Access to NATO NU/NR.

Standard Service Support Levels*:*

Service Availability Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP072 Core Financial System (CFS) Application Service

Service ID: APP072

Service Name: Core Financial System (CFS) Application Service

Portfolio Group: Application Service

Service Description: COTS-based service offering a system that supports standard & IPSAS financial processes used in NATO.

Value Proposition: Service configured to support project implementation and lifecycle for medium to large projects, thus enabling financial and accounting administration of projects in an effective and efficient manner.

Service Features: The service covers requisition, purchasing, project accounting, payments, General Ledger, and reporting. It supports standard financial, procurement, payment, and reporting functions belonging to a COTS-based financial system.

Service Flavours: The Service is available as a single flavour.

Available on: NR

Service Prerequisites: The Service requires virtual servers configured to enable functioning of the Oracle PeopleSoft Financials 8.4.

Standard Service Support Levels*:*

> **Service Availability *Target:*** 99.5%
>
> ***Service Restoration:*** Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.
>
> **N.B.** Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP074 NATO Lessons Learned Portal (NLLP) Application Service

Service ID: APP074

Service Name: NATO Lessons Learned Portal (NLLP) Application Service

Portfolio Group: Application Services

Service Description: The NATO Lessons Learned Portal Application Service supports the Lessons Learned communities in sharing and searching through lessons learned data, in tracking the progress of the staffing of observations, in managing the user accounts, roles and access, and in managing portal meta-data through a concept of data dictionaries. The Service supports NLLP managers, Lessons Learned Community of Interest (COI) site administrators, lessons learned facilitators, and regular NLLP users in:

- Tracking the progress on the NATO Lessons Learned process of specific observations;
- Managing the users and their access and rights to collaboration sites;
- Managing collaboration site metadata;
- Managing shared COI-specific collaboration sites with dedicated search metadata, with document libraries and event information.

Value Proposition: The Service is an essential enabler of a more effective and efficient NATO Lessons Learned process.

Service Features: The Service provides the following features to NLLP users:

- Creation and management of COI shared sites, including exercise event sites (NATO EXTRA COI);
- Management of metadata for COI shared site searches;
- Management of metadata for the lessons learned document searches;
- Integration with authenticated classified windows domain users;
- Management of membership users and roles;
- Access through forms-based solution;
- Assignment of users to NLLP application roles: site collection managers, NLLP managers, lessons learned facilitators, and NLLP users;
- Distinction of COI users into owners, members, and visitors;
- Facilitation of the NATO Lessons Learned Process workflow through:
  - Adding observations;
  - Maintenance of the lessons status;
  - Provision of the automated mail notifications;
  - Tracking of progress from noted, potential best practice, lessons learned, and best practice stage;
  - Archiving of lessons learned data;
- News pages;
- Conversion of the lessons learned data into PDF format documents to enable sharing;
- Storing and provision of the lessons learned documents;

- Management of specific site related to lessons learned related events and activities;
- Access to usage data collection datasets in a standardised and documented manner

Service Flavours: The Service is available in two flavours:

The full NLLP – includes all the features of the Service, including the tracking of lessons learned;

Public NLLP – includes all the features of the Service, except the tracking of lessons learned.

Available on:

NATO Unclassified
NATO Secret

Service Prerequisites:

Windows server 2016
SQL Server 2016
SharePoint Server 2016
IIS 8.5. for NCS users
WPS001 Managed Devices Service

Standard Service Support Levels*:*

Service Availability Target: 99.5%

Service Restoration: for NCS customers, the restoration priority will be as specified in centralised or local service level agreement.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP075 Electronic Warfare Functional Services (EW-FS) Application Service

Service ID: APP075

Service Name: Electronic Warfare Functional Services (EW-FS) Application Service

Portfolio Group: Application Services

Service Description: The EW-FS Application Service provides an integrated, robust, and flexible capability supporting a suite of services available throughout the Bi-Strategic Command (Bi-SC) Automated Information System (AIS) to address the NATO's emitter data management processes and dissemination of EW information in a timely and responsive manner in accordance with NATO policy, doctrine, and guidance. It is as a web-based capability, with advanced data storage, and near-real time data sharing capabilities, deployable in a federated infrastructure of system of systems. The Service includes Increment 1 of Electronic Warfare Functional Services (EW-FS), and it is implemented through the NATO Emitter Database – Next Generation (NEDB-NG) application. The capability can adequately describe modern complex emitters, which continue to proliferate within the electromagnetic environment and it supports the automation and integration with other information capabilities.

Value Proposition: The Service provides the NATO Electronic Warfare Community with a capability to achieve the following operational benefits:

- Support to NATO's emitter data management processes;
- Sharing of emitter information and data across NATO at all levels of command;
- Enhancement of the emitter information dissemination to Nations and other domains;
- Coordination between data providers through the Active Task mechanism;
- Contribution to the development of the initial Electronic Order of Battle (EOB);
- Provision of the search and analytical capabilities to retrieve/analyse emitter information;
- Provision of specialised functionalities in support of specific domains: radar electro optical and communication externals;
- Support to interoperability with external systems;
- Deployment in a federated infrastructure of system of systems, including classified networks and standalone machines;
- Management of Users and Permissions;
- Support to all operational mission types.

Service Features: EW-FS Application Service is comprised of the following features:

- Manage Emitters: support a user-friendly method of describing Emitters of Radar, EO/IR and Communications External (COMMS EX) types, platforms, weapons and site information and other waveform features belonging to modern multifunction emitters. Enable a realistic description of emitting modes built from discrete values, added with modulation details in sets and combined in a user defined sequence to a final Mode Line.

- Active Tasks: support NEDB-NG users to manage tasks related to emitters stored in the NEDB-NG. Within these Active Tasks there are two main groups: global and national.
- Manage Views: provide users of NEDB-NG with a user-friendly and intuitive interface to search, navigate and display emitters, emitting modes, platforms, weapons and site information.
- Query Builder: is a tool in the application which will allow the users to extract information of the NEDB-NG with the desired criteria.
- Manage users: support the management of user accounts and association of NEDB-NG with various roles and functionalities. The main roles associated with NEDB-NG are: System Administrator (SA), Database Manager (DBM), Database Administrator (DBA), and Database Provider (DBP).

Service Flavours: The EW-FS Application Service may be fully customized to provide different views supporting the following operational roles:

- NEDB-NG Database Manager (DBM);
- NEDB-NG Database Administrator (DBA);
- NEDB-NG Database Provider (DBP);
- NEDB-NG Database Reader (DBR);
- NEDB-NG System Administrator.

Available on:

NATO Secret

Service Prerequisites:

INF004 Infrastructure Virtualization Service

Standard Service Support Levels:

Service Availability Target: 99%

Service Restoration: In case of NEDB-NG failure, the interruption of services shall not exceed two hours in 80% of cases for an individual NEDB-NG User.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP076 Indications & Warnings (I&W) Application Service

Service ID: APP076

Service Name: Indications & Warnings (I&W) Application Service

Portfolio Group: Application Services

Service Description: The Indications & Warnings (I&W) Application Service provides a portal for the intelligence watch community, with a tool enabling monitoring of indicator statuses and sharing of warning intelligence.

Value Proposition: The Service provides the NATO Intelligence Community with a capability that enables management, access to, contribution, visualisation, reporting, and repository of relevant indicators.

Service Features:

- A comprehensive I&W indicators and reports search capability;
- Creation, upload, and management of warning reports;
- Color-coded Watch Conditions (WATCHCON);
- User-updatable indicators, sub-indicators, and their definitions;
- User-updatable links and supporting documents;
- User-configurable news and newsfeed system.

Service Flavours: The Service is available as a single flavour.

Available on:

- NATO SECRET
- BICES Network

Service Prerequisites:

- PLT001 Information Sharing and Collaboration Platform Services
- PLT003 Web Hosting Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP078 ORION Space Domain Application Service

Service ID: APP078

Service Name: Orion Space Domain Application Service

Portfolio Group: Application Services

Service Description: The Orion (Space Domain System) Application Service provides an integrated and flexible capability supporting Space Support in Operations services throughout the Bi-Strategic Command (Bi-SC) Automated Information System (AIS). Orion provides a centralised location for up-to-date Space Domain information (Space Domain Awareness), ensures the dissemination of operational Space support information (Operational Space Support) in a timely and responsive manner, and facilitates the coordination of Space actions with the other operational Domains (Space Domain Coordination), in accordance with NATO policy, doctrine and guidance.

Value Proposition: Orion provides the NATO Space Operational Community with a capability that enables the following operational benefits:

- Sharing of space support to operations data across NATO at all levels of command.
- Manage the dissemination of space support information.
- Provides an inventory of Space Assets and their capabilities, with search and analysis functions.
- Provides a system for Space-related information exchange supporting Space Domain Awareness (including Space threats), Operational Space Support and Space Domain Coordination.
- Provides a repository of Space-related documentation in support of the four lines of effort of the NATO Space Bi-SC Space Working Group (e.g., education initiatives, collaboration and engagement with National and international entities). Support interoperability with external systems.
- Manage Users and Permissions.
- Support all operational mission types.

Service Features: The Orion Application Service is comprised of the following features that combined support the three key tasks of the Space Operational Community:

- Provides a system to request, approve and monitor Space Support Requests (SSRs).
- Intelligence management. Provides the operational community with up-to-date Space-related intelligence information (including counter-Space).
- Intelligence Processing – creation/management of intelligence products on RED Space capabilities, such as Space Order of Battle (ORBAT)

Service Flavours: The Orion Application Service can be customized and adapted to the requirements of the operational community.

Available on:

NATO Secret

Service prerequisites:

WPS001 - Managed device service

Standard Service support levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP079 NATO Automated Biometrics Identification (NABIS) Application Service

Service ID: APP079

Service Name: NABIS Application Service

Portfolio Group: Application Services

Service Description: The NATO Automated Biometrics Identification System (NABIS) is designed to support the NATO Biometrics capability by enabling the user community to safely exchange biometric data in a NATO Joint Operations Area (JOA), between JOAs and beyond the operational context. The NABIS supports the full spectrum of the military operations, from tactical to strategic level, and can make a critical contribution to removing anonymity from threat actors.

Value proposition: Biometric capture and data interchange in the multi-national operational environment is something that has posed a great challenge to NATO operations. NATO has no effective means by which to assist the Nations to share data in a flexible yet interoperable way. NABIS has been developed to address and mitigate this shortfall, as follows:

- establishes a data sharing environment on the BICES/ NS WAN networks enabling the exchange of biometric data amongst participating NATO nations;
- enables and promotes biometric interoperability, biometric data sharing, as well as provides biometric capability for participating NATO nations that do not have their own national system;
- NABIS is a web application that allows storage, search, retrieval and dissemination of biometric data. It used a commercial engine to support automated matching of three modalities (Face, Fingerprint and Iris);
- it has an robust architecture, which can be easily extended with new functionalities or connections to other external matching engines;
- NABIS implements NATO STANAG 4715 compliant format for the exchange of data with other ABISs or enrolment devices and has functionality to import and export data from and to other biometric formats such as the USA Department of Defence (DoD) and Federal Bureau of Investigation (FBI) Electronic Biometrics Transmission Specification (EBTS).
- provides biometric and biographic data upload, which allows national ownership as defined in NATO standards (STANAG 6515 and STANAG 4715);
- uses web services to support “Ping and Ring” networks between multiple ABIS systems;
- provides a technical solution to manage Persons of Interest (PoI) included in the JOA Biometrics Enabled Watchlist (BEWL);
- supports the vetting process of the Locally Employed Personnel (LEP) in both static and deployed environments;
- contributes to Identity Intelligence (I2), Human Network Analysis in support of Targeting (HNAT), Force Protection and Counter Intelligence.

Service Features: NABIS is comprised of the following essential features:

- imports and stores biometric enrolments (i.e. fingerprints, face and iris) as well as latent prints from both collection devices and other ABISs;

- conducts automated searches of a newly imported/ received biometric file against the entire data base;
- performs an automated match/ no match decision based on pre-set thresholds and matching scores;
- provides a list of candidates sorted on the fused matching score, which supports further examination of face and latent images;
- it is NATO STANAG 4715 compliant;
- imports data from enrolment devices or other data collection and storage systems;
- shares biometric files through “Ping&Ring” transactions with networked ABISs, which allows for exchanging architecture where each participant retains the ownership of their data;
- enables management of PoI on the BEWL.

Service Flavours: NABIS supports Biometric Operations by storing, comparing, matching and disseminating three biometric modalities – fingerprints, face images and iris images. Within NABIS, data is grouped in two main categories based on how the biometric modalities have been collected: (a) enrolments, which includes the enrolled fingerprints, face and iris and (b) latent, which contains the latent prints collected from various objects. The NABIS also displays the JOA BEWL through a dedicated folder. The NABIS allows for advanced searches based on contextual information as well, and for saving the searches for accessing any potential updates. Likewise, it allows for subscriptions, which enables the user to be notified by emails whenever a new data matching the subscription was received in the system.

Available on:

NATO Unclassified (Training and exercise only)
NATO Secret WAN
BICES

Service prerequisites: NABIS is a fully web based application that requires a server installation. Client machines only require a HTML5 compatible browser like Chrome or IE11 or later.

Standard Service support levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP081 Joint Advanced Distributed Learning (JADL) Application Service

Service ID: APP081

Service Name: Joint Advanced Distributed Learning (JADL) Application Service

Portfolio Group: Application Service

Service Description: JADL Application Service and Support provides users across the Alliance the ability to access and deploy e-learning. In addition, it provides help desk services for all users.

Value Proposition: This service includes the offering of a Learning Management System (LMS) to NATO (-partner) Nations. By leveraging this platform (JADL, aka 'ILIAS'), users can decrease delivery costs and increase speed of delivery of online training. Moreover, JADL provides detailed analytics about the learning process, completions and scores of individual users, as well as groups. So by making use of JADL, customers can make sure their audiences are trained for a specific task faster, and for less money. Services include hosting the learning management system and managing the help desk for all users.

Service Features:

For end-users (individual learners):

- Provides access and consume e-learning modules
- Provides certificates after successful completion
- Provides helpdesk support to all users

For NATO entities (commands, Nations etc.) deploying online content on JADL

- Manages content on JADL
- Provides reporting and analytics

The helpdesk support will have the following characteristics (all included in one package, no cost differentiation between support levels):

- *Level 0: Self-service:*
  Guidance / micro-learning in JADL about basic features so users can trouble-shoot themselves, and prevent tickets in the first place

- *Level 1: Basic helpdesk support*
  Support basic issues in the start-to-end process: access, account request, approval, login, search for course, join course, course progress, certificates.
  Support more complex and non-standard issues + managing *content*, e.g. modules that won't play (troubleshooting and fixing needs to take place in the SCORM package /module itself, not in the LMS), uploading and testing new courses, removing obsolete content, generating reports for specific customers etc.

- *Level 2: Advanced help desk support*
  Support to solve deeper engineering issues in the platform itself.

Service Flavours: N/A

Available on:

NATO Unclassified

NATO Secret

Service Prerequisites:

WPS001 Managed Device Services for JADL on NATO Secret.

Standard Service Support Levels*:*

Service availability target: *99.0%* ***(TBC)***

Service Restoration: Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP082 Digital Emergency Alert Notification Service

Service ID: APP082

Service Name: Digital Emergency Alert Notification Service

Portfolio Group: Application Services

Service Description: The Digital Emergency Alert Notification Service provides customers with timely emergency alerts and mass notifications which can be sent to target audiences or broadcasted in mass to users on NATO Networks; as well, to the community members. The service enhances security and situational awareness with comprehensive enterprise class alerting essential to crisis response and civil communications.

Value Proposition: The service offers intelligent emergency communications distribution combined with guaranteed content delivery. Furthermore, it allows for the placement of methods, functions and triggers that interact with and bring crucial data to and from end-users; based on end-user and/or management's predefined business rules and settings. The Service provides seamless integrations with enterprise-class federated environments and shares communications and commands using standardized HTTPS, XML, HTML, SMTP protocols.

Service Features: The Service is installed as a client application on Managed Devices and when activated by "push" notifications from "notification moderators", the user receives a near real-time Pop-Up notification box where a pre-defined or custom tailored message can be seen. Includes a fully managed VM centrally hosted, a web-based server application solution secured with the appropriate posture for use on NATO Networks. The Service approach is based on applications that work in tandem with stakeholders to deliver a comprehensive solution.

Features and Options include:

- Templates: create and save alert templates for future use
- Scenarios: create alerts in advance for rapid activation manually or automatically
- Pre-scheduling of alerts for release at scheduled date and time
- Scheduling of recurring alerts
- Built-in capability for scrolling banner text computer alerts
- Sizing of computer alerts from small to full screen display
- Text-to-voice feature automatically reads the computer alert out load
- Each user may have multiple email addresses, multiple phone numbers, multiple SMS numbers, multiple keywords, multiple groups, multiple roles

Service Flavours: The service is offered as a single flavour.

Activities in scope of service:

- Service management of entire service lifecycle including regular user communication;
- Requirements analysis and validation with the customer:
    - Propose technical solution;
    - Evaluate and propose costs based on requirements and technical solution;
- Application management:

- Incident Management:
  - Issue Investigation and Resolution; Escalation of tickets to 3rd party supplier when required and follow up until their final resolution;
- Independent Verification & Validation:
  - Change Configuration Proposal (CCP) Submission and Follow up;
- Deployment:
  - Configuration & Reconfiguration;
  - Deploying & Release, and Patches Management;
- Operations:
  - Operate and perform the required maintenance on the application servers and the underlying platform;
  - Set up and Maintenance required Reference/Test and Development environment in NSF and make it available for the customer.

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Public Cloud

Service Prerequisites:

WPS001 Managed Device Services

WPS002 Enterprise Identity Access Management Service

WPS016 Enterprise Managed Mobility Service

Standard Service support levels:

Service Availability Target: N/A

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the service is ‘per managed device’. Please see Service Rate document for the price details.

APP083 Mission Planning Application Service for Dual Capable Aircraft

Service ID: APP083

Service Name: Mission Planning Tool for Dual Capable Aircraft

Portfolio Group: Application Service

Service Status: Available

Service Description: The Mission Planing Tool for Dual Capable aircraft provides computer tools to aid in planning conventional and non-conventional aircraft missions. It will be based on the Joint Mission Planning System (JMPS), and will consist of computer hardware using common core software called the Joint Mission Planning Environment (JMPE). JMPS is intended eventually to support most aircraft, weapon, and sensor assets. This Service includes the maintenance of relevant operational support data e.g. maps, Digital Aeronautical Flight Information File and aircraft performance profiles.

Value Proposition: This Service will allow the user to plan conventional and non-conventional aircraft missions. It will provide a package of common and platform-unique mission planning applications that will help to increase the accuracy of the military planning cycle and will improve combat readiness.

Service Features:

- Operational Scenario management
- Pre-mission briefing
- Route planning and evaluation
- Target / objective analysis

Service Flavours:

- Stand-alone workstation
- Network based installation (VDI)

Available on: NATO Secret

Service Prerequisites: WPS001 Managed Devices

Standard Service Support Levels*: (std)*

Support Hours:

Centralised Service Desk specialist agents are available during:

- Monday to Thursday: 0600 to 2200 (CET)
- Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial numbers:

Belgium +32 65 44 3177
Netherlands +31 70 374 3177
Italy +39 081 721 3177
Germany +49 282 4978 3177
USA +1 757 747 3177
For NATO HQ +32 02 707 5858

Service Availability Target: 99.5% Availability

Service Restoration:

Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. *Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.*

Service Cost / Price: The unit of measure for the Service is 1. Service Initiation and In-Service-Support will be provided and charged in accordance with the scope and financial estimates developed and agreed through site specific Technical Agreements.

APP084 International Submarine Escape and Rescue Liaison Office (ISMERLO) Application Service

Service ID: APP084

Service Name: International Submarine Escape and Rescue Liaison Office (ISMERLO) Application Service

Portfolio Group: Application Services

Service Description: ISMERLO is a web based Command & Control system used to plan and co-ordinate escape and rescue efforts for the worldwide submarine community during peace time.

Value Proposition: The system enables the international submarine community to manage all submarine escape and rescue assets and elements. It enables the community to raise alerts for real or simulated submarine incidents and to help determine the quickest and most effective escape and rescue assets to use to assist with the escape or rescue activities.

Service Features:

- Time to First Rescue and Time to First Intervention C2 planning calculations.
- Real world navigational routing for support vessels.
- Vessel position updates via AIS
- SMS and email notifications of real world alerts and exercises.
- Vessel of Opportunity management.
- Submarine management.
- Rescue and intervention asset management.
- Airport & Seaport data management.
- Medical data management.
- Private and group communications.
- Forum, event and calendar management.
- Site data managed and maintained through comprehensive integrated Content Management System.

Service Flavours: One version of the system is available.

Available on: The system is available on the open internet. This is because the ISMERLO community is made up of all worldwide nations that have submarine capabilities. This includes NATO members, and also nations such as Russia, China, India and Australia etc.

Service Prerequisites: No prerequisites needed.

Standard Service Support Levels*:* P3 level

All supporting and underpinning services for ISMERLO are expected to carry at least a 99.8% availability.

Service Cost / Price: The unit of measure for each of the Service Flavours is 1. The total of the NATO Service Delivery cost is charged in accordance with specifically arranged conditions of the Service Delivery.

APP085 Housing Office Management Application Service

Service ID: APP085

Service Name: Housing Office Management Application Service

Service Type: Customer Facing

Portfolio Group: Application Service

Service Status: Available

Service Description: The Service offers our Customers an improved and effective Housing Management solution that supports properties managed by local Housing Offices, both on-base and off-premise properties, allowing consolidated management of leases and coordinate maintenance requests.

Value Proposition: The Housing Office Management Application Service serves the property management and rental flow for NATO military and civilian personnel entitled to rent on base housing in an automated and standardized manner.

Service Features: Housing Office Application includes the following Modules:

- **Register customer application** - Customer application form management and printing;
- **Customer Administration** – Search Customer; List Customers; Edit Customer Details; Add customer to waiting list; Print customer validation form;
- **Residence Administration** - Register residence; Search residence; List residence on criteria; Edit residence details;
- **Proposals Administration** - Register proposal; Print proposal/offer from template; Search customer proposals; List proposals;
- **Booking Administration** - Register booking; Print acceptance from template; Search customer bookings; List Bookings;

Service Flavours: The Service is available as a single flavour.

Available on: NATO Unclassified.
The Service may be available on other security domains upon a New Service Request.

Service Prerequisites:
WPS001 Managed Device Service
WPS002 Enterprise Identity Access Management Service

Standard Service Support Levels:

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period is 8 hours.
N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is by a Database instance. Price details available in the Service Rates Document.

APP086 NATO Information Portal Application Service (NIP)

Service ID: APP086

Service Name: NATO Information Portal Application Service (NIP)

Portfolio Group: Application Services

Service Description: The Service provides a secure, online collaborative environment for users to create, capture, store, manage, broadcast, publish, view, and search all types of digital content. It allows organizational elements to establish an Intranet rich collaboration environment by utilising and combining web information publishing and portal feature options. This Service is interoperable with an existing Tasker Tracker Application Service (APP030) and an existing Enterprise Document Management Application Service (APP031), but also deployable as standalone Service.

Best for: portals that require high volumes of information frequently updated to be pushed to users and native integration with EDMS and/or TT+.

Value Proposition: The Service allows users to work together much more effectively by sharing information, jointly working on documentation. Users are able to publish content directly, without the intervention of a webmaster. The offered collaboration and social services are an enabler for an effective Information Knowledge Management (IKM) within a controlled information lifecycle, in compliance with NATO IM Policies, and protected.

Service Features: The Service provides the following features:

- **Dashboard**: a standard landing page for each Command.
- **Command Structure**: implementation of the Command Structure to navigate the NIP and reorganization driven by metadata.
- **Dedicated Command Page**, with Alert State and Footer links categorized by groups.
- **Site Templates**: Landing page, Document Collaboration, Exercise, etc.
- **Events Management**: approval workflow for publishing on Command page, events sharing across Commands and Departments, conference room management, bookings & attendees management with notifications and calendar functionalities using Exchange, registration lists to events.
- **Articles Management**: Command page publishing approval workflow, articles sharing across Commands and Departments.
- **Data and Information Management**: Countries, Key Individuals and Organizations**,** Exercises & Operations**,** Training.
- **Enforced Classification of Information**: Highest classification displayed on each page according to the information item highest classification.
- **Search Centre**: Search using refiners supporting information discovery.
- **Bi-Strategic Commands IKM Change Management Board (BICMB)**: change request management tool driving the continuous improvement of the IKM Tools.
- **Optional integration with EDMS**: documents displayed on Command Page, Departments, Nations and Community.
- **Optional integration with Tasker Tracker Plus (TT+)**: Taskers displayed on Command page from Command TT+, Taskers assigned to their respective office displayed on their respective Department/COI pages.

Service Flavours: The Service is available as a single flavour.

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret
NATO Partner network (For NNHQ)

Service prerequisites:

WPS002 Enterprise Identity Access Management Service
WPS003 Enterprise User License Service
PLT003 Web Hosting Service

Standard Service Support Levels:

Service Availability Target: 99%

Service Restoration Priority: P2.

The Standard Service support comprises the following activities:

- **Operation**: application monitoring, log management, batch jobs management, backup & restore, auditing, Service Requests fulfilment.
- **Corrective Maintenance**: diagnosis and removal of the causes and the effects of any malfunction affecting the Service.
- **Preventive Maintenance**: preventive actions needed to avoid future malfunctions
- **Adaptive Maintenance**: adjustment of the Service in order to adapt to the minor changes of the sub system components (i.e. Operating System, Database Management System, Browser, SharePoint and SharePoint add-ons). Major changes of the sub system components shall be requested via dedicated projects.
- **Minor Perfective Maintenance**: development of up to one minor enhancement[1] of the Service per month[2] (only applicable to the NIP Service Flavour). Development of up to one complex Business Intelligence (BI) report[3] per year.

Service Cost / Price: The unit of measure for the Service is “per user”. Since the Service is designed for the general use by all the users of each customer, the number of user will be assumed to be equal to the sum of the “NATO Peacetime Establishment (PE)” users plus the “NATO Non-Peacetime Establishment (NPE)” users.

[1] A “minor enhancement” is defined as a limited change of an existing functionality or the creation of a new functionality of the Service, that requires in total not more than 5 man days in order to be designed, developed and tested. All the enhancement requests shall be vetted and prioritized by the “Bi-SC IKM Change Management Board” before being developed.

[2] This activity will be paused during major implementation projects affecting the Service.

[3] A “complex BI report” is defined as as a report that requires in total not more than 15 man days in order to be designed, developed and tested. The report can fetch data from the NATO Information Portal (APP086), but also from the Tasker Tracker Plus (APP030) and the Enterprise Document Management System (APP031). All the requests for new reports shall be vetted and prioritized by the “Bi-SC IKM Change Management Board” before being developed.

Each instance of the Service should be counted separately (so for example, if the same user is using two different instances of the Service on two different networks, the user should be counted twice).

The cost of the Service does not include the cost of all the underlying Service prerequisites.

The total amount of the Service delivery price is charged in accordance with specifically arranged conditions of the Service delivery.

APP087 CRC System Interface (CSI) Application Service

Service ID: APP087

Service Name: CRC System Interface (CSI) Application Service

Portfolio Group: Application Services

Service Description: The NATO Control and Reporting Centre (CRC) System Interface (CSI) is a real time Command & Control System currently in operational use in 26 NATO nations. The system, originally developed by Raytheon, has since been significantly modified and enhanced under the multi-nationally funded CSI Memorandum of Understanding. The legacy hardware has been replaced by modern Common off the Shelf (COTS) hardware and the software has been totally re-written to support today's modern operating systems.

The CSI System is used both as a Command & Control system and as a Data Link Integrator, integrating both radar feeds and tactical data links. All major data links are supported including Link 1, Link 11A, Link 11B, Link 16, ATDL-1, Variable Message Format (VMF), Cursor on Target (CoT), OTHT-Gold and NATO Friendly Force Interface (NFFI).

The CSI offers integrated fighter control for directing Link 16 equipped fighters and full Ground Based Air Defence (GBAD) control. The Human Machine Interface (HMI) is a modern Java application that can either be deployed standalone or as part of an integrated MASE / CSI solution.

The CSI Local Support Service flavour includes the installation, configuration and maintenance by the CSU Staff of the CSI system in order to facilitate the 24/7 availability of the system for the operational staff at NCS Sites. A detailed description of these particular activities can be found under "Service Flavours" below

Value proposition: The CSI server is the main application. It is developed in Ada and C and provides most of the CSI System functionality.

CSI is a real time Command and Control system interfacing on ATDL-1, Link 1, Link 11A, Link 11B, Link 16, OTH-Gold, NFFI, VMF and COT. The CRC Systems Interface provides complete SAM, Link16 C2 Unit and Fighter control (Link 16 Non-C2 Air Unit) functionality into the CRCs, provides a correlated air, ground, surface, subsurface, and space picture for SAM units, Fighters, the E3A, ships, CRCs and other land units.

The primary purpose of CSI is to provide CRCs with a Fighter control and SAM control functionality and to route tactical data to any connected system. The CSI implements Threat Evaluation and Weapon Assignment (TEWA) processing; it is able to evaluate a list of the most threatening tracks against the points to be defended and it associates the best SAM/Surface system for the engagement.

The TEWA processing has been applied to fighter control in addition to GBAD control. It is possible to draw Safety Sectors and Factor Bandit Range Sectors around hostile and friendly tracks. These sectors represent the engagement volume of the fighters. Time to safety sector and time to factor bandit range inform the fighter controller about crucial timing related to fighter interception.

CSI implements pre ID and auto ID functionality based on Link 16 identities. It also implements a procedural identification evaluation based on the loaded ACO corridors.

The CSI uses the standard NATO data links Link-1, Link-11A, Link-11B, ATDL-1, Link-16 and OTH-Gold. Data exchange between the CSI System and the CRC is accomplished via the Link-1 protocol, Link 11B protocol or Link 16 protocol. This is site dependant and depends upon the interfaces provided by the host CRC. Data exchange with connected units is accomplished via Link-16, , Link11B, Link11A, ATDL-1 or OTG. Data exchange between the CSI and fighters is via the Link 16 protocol only. The CSI acts as a message translator between interfaced systems and provides the necessary communication gateway services required to reconcile incompatibilities between the referenced links.

CSI fully supports the latest Network Enabled Weapons functionality.

CSI can run in a redundant configuration where two servers are running simultaneously, one as master and one as slave. The slave server is in hot standby mode and at the event of a catastrophic failure of the master server, it takes over migrating all the connections.

Service Features: The CSI supports many different simultaneous connections (Link 1, Link 11A/B, ATDL-1, VMF, Link 16, JREAP, NFFI and OTHT-Gold). For Link 16 the CSI has everything to operate both on a live Link 16 network and to connect to other Link 16 systems using normal ground infrastructure. The HMI has been completely re-designed based upon state-of-the-art techniques and tools. The functionality within the CSI system includes:

- Transmitting/Forwarding and Receiving of tactical datalink messages

  (Link 16, Link 11A, Link 11B, ATDL-1, Link 1, VMF, NFFI, CoT)
- Reception and forwarding of Over the Horizon Target Gold (OTHT-Gold).
- Pre ID and auto ID functionality based on Link 16 identities.
- Procedural Identification Evaluation (PIE) based on the loaded ACO corridors
- Track processing for Air Tracks, Surface tracks, Land Tracks, Subsurface Tracks, Reference Point, Emergency Points, EW Products and Space Tracks.
- Correlation/De-correlation (Air Track/Air Track, Air Track/Target, TBM/TBM)
- Filtering (Geographic/Identity/Security)
- Online Tactical Data Extraction and Monitoring
- Free Text Message exchange
- Link-16 Imagery Processing
- Link-16 Network Enabled Weapons
- Recording/Reduction and Replay
- SAM/GBAD Control and Monitoring
- Fighter Control (STANAG and MilStD) and Mission Monitoring
- TBM data provision, processing and engagement management from Link 16 and connected radars (TPS-77, RAT-31DL and SMART-L)
- Link 16 exchange on an unlimited amount of connections using various protocols (e.g. MIDS/JTRS (A, B, I, D, J, R, MOS) over Ethernet or 1553 Bus, JREAP and SIMPLE)
- Advanced JREAP (A,B and C) routing including (remote) management messages

- Multiple MIDS LVT (1,2,4,6,11) BU1, BU2, STT and JTRS Terminal Monitoring and Control
- CSI Integrated Link 16 Network Management Application (CINEMA)
- Link16 Network and Terminal Emulation
- Link 16 network design through CSI Advanced Network Design Tool (CANDIT)
- Local and Remote Link 16 Ground Equipment Suites.
- NTDS Interface Processor (NIP) for communication on Link 11A.
- Flight Plan Receiver / Flight Plan Server (From MASE Repository)
- ATO/ACO automatic and manual reception and processing.
- Threat Evaluation and Weapons Assignment (TEWA) for SAM units and fighters.

Service Flavours:

CSI software maintenance and in service support: (singleton service provided to Members of the CSI Board) Includes the development, testing, documentation and release of the CSI baseline to all sites registered for CSI. However, the sites themselves are responsible for the system update.

CSI instance installation and in service support: Upon request, CSI instances can be provided to CSI Board Members through an installation service. Such services are requested through a Customer Request Form and implemented via a Technical Agreement to be funded by the service requester.

CRC System Interface (CSI) Local Support Service (INF041): The following services are provided under NCI Agency CSU Support:

1) Installation of new baseline

NCI Agency CSI section releases annual baseline updates to CSU’s after the baseline has been accepted on the Approved Fielded Products List (AFPL). Upon release of a new baseline, CSU personnel will perform the baseline upgrade to install the new version of the CSI Software.

2) Adding / Modifying connections to the system

The addition of connections and the modification of connections are usually performed by CSI System Operators. However, liaison will be required with CSU personnel to ensure that the correct route exists to the connecting system and that the connection can successfully pass through any established firewalls.

3) Troubleshooting connections

Connections employed in the CSU consist predominantly of JREAP-C and Link 11B connections. Occasionally a channel may be in the failed status and CSU personnel may be requested to diagnose the data link issue to determine which system is at fault.

4) Data Archiving.

All data exchanged by the CSI System is recorded. In addition, the operational picture and operator inputs are also recorded. CSU personnel are responsible to ensure that all data (including operational logs / system logs) are correctly archived for any future use.

Value Proposition: Use of the CSI Local Support service provides for a reliable CSI installation allowing data to be exchanged between NATO installations and national sites. The use of the service ensures the availability of the CSI system, ensures that the baseline being run is the latest available version on the AFPL and ensures that physical connections are correctly established in order to serve the data exchange requirements.

Service Features: The functionality within the CSI Local Support includes :

- Baseline installation
- System configuration
- Data Archiving
- Datalink troubleshooting

Available on:

NATO Confidential
NATO Secret
Mission Secret
The Service may be available on other networks upon a New Service Request.

For INF041, CSI Software is delivered as a NATO Restricted delivery. The installations supported by the CSI Local Support service are hosted solely on the NS-WAN.

Service prerequisites:

WPS001 Managed Device Service

For INF041, the CSI runs on virtual machines provided by the CSU and therefore these virtual machines need to be available to support the CSI Local Support Service

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

- Monday to Thursday: 0600 to 2200 (CET)
- Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 CET).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

Belgium +32 65 44 3177
Netherlands +31 70 374 3177

Italy +39 081 721 3177
Germany +49 282 4978 3177
USA +1 757 747 3177
For NATO HQ +32 02 707 5858

Service Requests:

To request this service please complete the Customer Request Form and contact NCI Agency Demand Management. https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

The overall CSI availability target (99.5% yearly) is calculated as the combined availability of all of the following components (user identifiable functions):

CSI functional component	Target Availability	Performance threshold (initial access time)	Remarks
CSI Server Application (CSA)	≥ 99.5%	30”	Administrators should be able to load the CSI Server Application (MSA) within 30 sec.
CSI Console Application (CCA)	≥ 99.5%	20”	User should be able to access CSI Console Application (CCA) within 30 sec.

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 1 hour.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service flavours is listed in the table below. Where the unit of measure is states as n/a, the service Initiation and In-Service-Support will be provided and charged in accordance with the scope and financial estimates developed and agreed through site specific Service/Technical Agreements.

Service ID	Service Name	Service Flavour/Option	Service Unit of Measure
APP087	CSI Application Service	CSI software maintenance and in service support	n/a

Service ID	Service Name	Service Flavour/Option	Service Unit of Measure
APP087	CSI Application Service	CSI instance installation and in service support	n/a
INF041	CSI Local Support Service	Support delivered to CSI at NCS Units by local Staff (CSUs)	per instantiation

APP088 CINEMA (CSI Integrated Network Monitoring and Management Application) Service

Service ID: APP088

Service Name: CSI Integrated Network Monitoring and Management Application (CINEMA) Service

Portfolio Group: Application Services

Service Description: CINEMA is an operationally proven Link 16 network monitoring and dynamic network management solution.

L16 Network management enables efficient use of the available bandwidth and provides alerts on inadvertent misuse of the frequency spectrum and violation of FCA regulations. Cinema addresses these needs using flexible solution.

The CINEMA runs on standard/COTS Windows PC or Solaris Workstation.

Value proposition: The CINEMA Service provides its users with the following number of key benefits:

- L16 Network Monitoring
  Enhanced Link 16 network monitoring capabilities sufficient to assure conformity with the nations' Frequency Clearance Agreement (FCA) requirements

- L16 Dynamic Network Management
  Reconfiguration of platform time slot assignments in real-time in case of over-loaded platform, under-utilised network capacity. Reconfiguring the assignments within the network design assures the intended tactical data information exchange

- Terminal Monitoring & Control
  Provides a flexible solution that can be set-up to monitor and control of a single-terminal network up to a multi-terminal/multi-network infrastructure with numerous remote MIDS sites.

Service Features: The CINEMA Service is comprised of the following features:

- Monitor and control L16 ground equipment suites/MIDS terminal(s).
  - Supports direct (over WAN) connection to the MIDS/STT having the Platform D/J/R interface.
  - Supports terminal discrete control(Power Off/On/Standby)
  - Initialisation, control & monitoring of local and remote terminals
- Monitor Link 16 Network(s)
  - Network participation monitoring
  - Time slot monitoring
  - Operational Network Plan and network design compliance monitoring
  - Link-16 messages monitoring
  - Frequency Clearance Agreement (FCA) compliance monitoring

- Guarding against ATC/Nav-aid interference within commercial airspace
    - Timeslot utilisation monitoring
    - Time slot duty factor (TSDF) monitoring
        - on individual platforms
        - on platform centric areas
        - on user defined areas
        - on a position
- Dynamic network management of networks and platforms
- Free text message(J28.2 and ANFT) capability
- User friendly HMI and Situational Awareness (SA) display
- Recording and reporting

CINEMA Server– Cinema Server is the server-application that establishes connection to the terminals and processes the Link 16 data. The server is running headless.

Cinema Console– Cinema Console is the user interface of the server. One server application can serve multiple console applications. The communication between the server and the console is done via a powerful MongoDB database, which is also used as a storage for the recordings and the Link 16 data.

Service Flavours:

CINEMA software maintenance and in service support: (singleton service provided to Members of the CSI Board) Includes the development, testing, documentation, release of the CINEMA baseline to all sites registered for CSI. However, the sites themselves are responsible for the system update.

CINEMA instance installation and in service support: Upon request, CINEMA instances can be provided through an installation service to customers of the CSI Board. Such services and related support are requested through a Customer Request Form and implemented via a Technical Agreement to be funded by the service requester.

Available on:

NATO Confidential
NATO Secret
Mission Secret
The Service may be available on other networks upon a New Service Request.

Service prerequisites:

WPS001 Managed Device Service

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

Monday to Thursday: 0600 to 2200 (CET)
Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 CET).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

Belgium	+32 65 44 3177
Netherlands	+31 70 374 3177
Italy	+39 081 721 3177
Germany	+49 282 4978 3177
USA	+1 757 747 3177
For NATO HQ	+32 02 707 5858

Service Requests:

To request this service please complete the Customer Request Form and contact NCI Agency Demand Management. https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

The overall CSI availability target (99.5% yearly) is calculated as the combined availability of all of the following components (user identifiable functions):

CINEMA functional component	Target Availability	Performance threshold (initial access time)	Remarks
CINEMA Server Application (CSA)	≥ 99.5%	30”	Administrators should be able to load the CINEMA Server Application (CSA) within 30 sec.
CINEMA Console Application (CCA)	≥ 99.5%	20”	User should be able to access CINEMA Console Application (CCA) within 30 sec.

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 1 hour.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: There is no standard service rate for the service flavours. Service Initiation and In-Service-Support will be provided and charged in accordance with the scope and financial estimates developed and agreed through site specific Technical Agreements.

APP089 Tasking, EXploitation and Assessment System (TEXAS)

Service Retired.

APP091 CSI JREAP Router Application Service

Service ID: APP091

Service Name: CSI JREAP Router Application Service

Portfolio Group: Application Services

Service Description: The JREAP Router is a software-based tactical data link (TDL) solution that enables data forwarding between multiple Link 16 networks over the JRE interface.

The JREAP Router runs on standard/COTS Windows PC or Solaris Workstation, and can either be run as a desktop application (with HMI), or as an operating system service. Software is used for enabling exchange, filtering, and routing (forwarded/relayed) of Link16 j-series messages (i.e. tactical picture) over the Joint Range Extension (JRE) Application Protocol (JREAP) among (near) real-time C2 systems.

With the JREAP Router software, it is possible to connect to a configurable amount of JRE endpoints. A “JRE endpoint” is simply a piece of software, which is located at Command and Control (C2) systems that have access to both Link 16 and alternate communications media (e.g., SATCOM, Fiber Optic, Land Line, or any combination of these or other communications networks).

The tactical picture received from connected JRE endpoint(s) could be forwarded to other JRE endpoint(s). While this forwarding is taking place, it is possible to apply JREAP tactical filters that can be used to reduce the amount of traffic that is being exchanged.

Value proposition: The JREAP Router Application Service provides its users with the following number of key benefits:

- Operate geographically dispersed units.
- Provide reach back to tactical picture from higher/rear C2 nodes/echelons.
- Overcome the requirement to necessarily provide dedicated airborne MIDS/JTIDS relays when their deployment would not be possible.
- Provide Link 16 data communication between surface / ground units when no airborne relays are available.
- Provide backup communications in the event of the loss of the normal link.
- Provide a connection to a platform that may not be equipped with the specialized communications equipment for that TDL.

Service Features: The JREAP Router software offers a configurable amount of channels (32 by default), each of which could be designated to support either of the following communication protocols, so as to support communication over either JREAP Appendix C (TCP/IP), Appendix B (Serial, Synchronous or Asynchronous), Appendix A (Announced Token Passing):

The JREAP-C interface/protocol supported is based on Internet Protocol (IP) (User Datagram Protocol (UDP) Unicast, and Transmission Control Protocol (TCP)).

The JREAP-B interface/protocol supported is based on Full-Duplex Synchronous and Asynchronous Point-to-Point.

The JREAP-A interface/protocol supported is based on Half-Duplex Announced Token Passing.

The JREAP Router receives Link16 data via its channels. The data received, could be filtered, and forwarded/routed within its channels.

The JREAP Router enables the user to visualize the received and/or transmitted picture per channel on a geographical display.

The JREAP Router provides On-line and Off-line data extraction capabilities of all messages exchanged on all channels.

JREAP Router exists in the following configurations:

JREAP Router Standalone – A lightweight self-contained version of the JReapRouter without the need of a database ideal for use on mobile platforms.
JREAP Router Client/Server – A client/server version. The server is running headless and the communication between the server and the client is done via a powerful MongoDB database which is also used as a storage for the tactical data link messages.

Service Flavours:

JREAP Router software maintenance and in service support: (singleton service provided to Members of the CSI Board) Includes the development, testing, documentation and release of the JREAP Router baseline to all sites registered for CSI. However, the sites themselves are responsible for the system update.
JREAP Router installation and in service support: Upon request, JREAP Router instances can be provided through an installation service. Such services and related support are requested through a Customer Request Form and implemented via a Technical Agreement to be funded by the service requester.

Available on:

NATO Restricted
NATO Confidential
NATO Secret
Mission Secret
The Service may be available on other networks upon a New Service Request.

Service prerequisites:

WPS001 Managed Device Service

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

- Monday to Thursday: 0600 to 2200 (CET)
- Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 CET).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

Belgium +32 65 44 3177
Netherlands +31 70 374 3177
Italy +39 081 721 3177
Germany +49 282 4978 3177
USA +1 757 747 3177
For NATO HQ +32 02 707 5858

Service Requests:

To request this service please complete the Customer Request Form and contact NCI Agency Demand Management. https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

The overall CSI availability target (99.5% yearly) is calculated as the combined availability of all of the following components (user identifiable functions):

JREAP Router functional component	Target Availability	Performance threshold (initial access time)	Remarks
JREAP Router Server Application (JSA)	≥ 99.5%	30”	Administrators should be able to load the JREAP Router Server Application (JSA) within 30 sec.
JREAP Router Console Application (JCA)	≥ 99.5%	20”	User should be able to access JREAP Router Console Application (JCA) within 30 sec.

Service Restoration: Where the service is deemed unavailable the service restoration period for a critical incident (i.e. P0/P1) is 1 hour.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: There is no standard service rate for the service flavours. Service Initiation and In-Service-Support will be provided and charged in accordance with the scope and financial estimates developed and agreed through site specific Technical Agreements.

APP092 Ship-Shore-Ship Buffer (SSSB) Application Service

Service ID: APP092

Service Name: Ship-Shore-Ship Buffer (SSSB) Application Service

Portfolio Group: Application Service

Service Description: The Ship-Shore-Ship-Buffer is a flexible, low-cost, state-of-the-art solution to support the communication between Air Defence Ground Systems, Maritime Forces and Airborne Early Warning via Tactical Data Links.

The SSSB system consists of a server and a client application which run on Commercial-Off-The-Shelf (COTS) platforms. The Buffer Operational Server (BOS) is the server application and the SSSB Console (CONS) is the client application. The data connection between server and client application is extremely efficient and allow the use of the client in local and remote mode using low bandwidth communication lines without any degradation of the user experience.

The SSSB server and client applications implement a sophisticated scripting language which allows full automation of user operations and training scenarios. Additionally the synchronization scripting commands and the support of distributed architectures allows the SSSB server and client applications to be used for TDL training and TDL testing.

The SSSB Server and client applications have been developed completely using the JAVA programming language to allow not only to support all the available hardware and software platforms but also to achieve a very short time in implementing enhancement and corrections as required by the SSSB user's community.

Part of the SSSB System products there is the Open-System-Communication-Control (OSCC) system which provides full control of communication equipment. OSCC is a client/server application which runs on COTS platforms. OSCC support already more than 50 communication equipment which range from radios (transmitters, receivers and transceivers), matrices (antenna, analogue and digital audio), Data Terminal Sets (DTS), discrete signals etc. Additional equipment can be added also by third parties using the OSCC Software Development Kit (SDK).

OSCC, for its distributed design, can support local and remote connections, full or limited access to equipment parameters from users with different authorization rights.

OSCC integrates VoIP/RoIP functions for voice coordination and to connect to military and civilian telephone networks.

The NCI Agency has developed specific Diagnostic Tools to assist the troubleshooting of TDL communication problems. The SSSB Diagnostic Tools can be used either by site personnel or by NCI Agency personnel when in depth troubleshooting is required.

The NCI Agency's AMDC2 offers a number of services for utilizing and supporting SSSB in operational and training environments and provides other services related to SSSB such as Management and Engineering support. A high level overview of offered services for SSSB is presented within the following chapters, a detailed description is provided in the SSSB MOU document.

Value proposition: The software products of the SSSB family provide a complete and integrated set of state of the art applications that enable the users to apply full control of:

- Tactical Data Link channel resources;
- Tactical Data Link Networks management;
- Voice coordination channels and;
- Communication equipment control and monitoring.

The technology insertions developed by the NCI Agency for the SSSB System has resulted in the definition of a new architecture for the deployment of the NATO SSSB Modernization Project based on IP interfaces to allow a flexible use of local and remote resource among all NATO SSSB installations.

SSSB provides a migration path from Link 11 to Link 22 supporting mixed Link 11/22 environment. The migration support covers all the Link 22 aspects from TDL messages, Network management, radio resources, TDL interoperability, communication monitor and troubleshooting.

Service Features: To assist the SSSB users in gaining and maintaining the Tactical Data Links communication the following areas are supported:

- Tactical Data Link formats: Link 1, Link 11, Link 11B, Link 22, JReaP;
- Non-Tactical Data Link formats: AIS (Automatic Identification System);
- Tactical Data Link transports: SIMPLE;
- Maintaining and exchanging of a real-time Recognised Air, Surface and Subsurface Picture (RASSP) based on TDL and non-TDL inputs;
- Controlling and monitoring Link 11 and Link 22 TDL Networks;
- Controlling and monitoring local and remote communication equipment associated to the TDL channels: Antennas, Radios, Switching Boxes, Modems, and Multiplexers etc.;
- Diagnosis of TLD communication infrastructure.

Service Flavours: SSSB is provided as a singleton service to the members or the SSSB Board. This singleton service includes:

- System Engineering support,
- Post design services,
- Documentation,
- Project management,
- Training support,
- Configuration management,
- Troubleshooting for communication,
- Maintenance and supply support,
- Transportation,
- Procurement and
- Quality and safety assurance.

Available on:

NATO Secret
Mission Secret

Service Prerequisites:

SSSB relies on an infrastructure able to host SSSB applications and enabling intra and inter-site data exchange through networking services.

PLT013 – NATO Integrated Secure Platform can be utilised to run SSSB application on a secured Solaris or Linux platform as required.

Serial Link 1 connections require that inter CRC infrastructure exists allowing the transport of serial data. SSSB support dedicated serial lines and virtual serial lines over network connections.

Link 11 connections require local and/or remote HF/UHF radio infrastructure, Data Terminal Set modem and Link 11 cryptographic equipment. SSSB provides direct support of all existing format of DTS models and interfaces as well as Link 11 cryptographic equipment. SSSB support both dedicated and IP communication for remote Link 11 infrastructures.

Serial Link 11B connections require secure connections with the remote systems. SSSB supports dedicated serial lines and virtual serial lines over network connections.

AIS connections require either a dedicated receiver or a connection to a National AIS concentrator facility. In the latter case, due to the different security levels, it is mandatory the use a serial diode between the systems.

SIMPLE connections require secure lines. Generally the SSSB SIMPLE ports are connected to the CFBLNet or NATO WAN networks.

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

- Monday to Thursday: 0600 to 2200 (CET)
- Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Ops Centre personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 CET).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

- Belgium +32 65 44 3177
- Netherlands +31 70 374 3177
- Italy +39 081 721 3177
- Germany +49 282 4978 3177
- USA +1 757 747 3177

- For NATO HQ +32 02 707 5858

Service Requests:

To request the SSSB Application service or related information, please complete the Customer Request Form and contact NCI Agency through the submit function included in the form following the link below. https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

The support provided by the NCI Agency for the SSSB system covers so many areas that a list of all the applicable key metrics will not provide any additional value. The Key Metric that can summarize all of them is the one that measure the grade of implementation of the Program of Work (PoW), as agreed by the Participants to the SSSB MOU.

Table 1: SSSB PoW Implementation

Indicato r	**PoW Implementation**
Description	This indicator measure the level of implementation of the PoW activities agreed the SSSB Board (Participants to the SSSB MOU). The PoW is a mixed set of Common Activities, like Software Maintenance, and Had Hoc Activities.
Measurement Method	Measuring the percentage of implementation of PoW activities.
Unit	%
Algorithm	Difference between actual and estimated man power
Target	Metric ≥ 85%
Applicability	All PoW entries

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: There is no standard service rate for this service. The total of the Service delivery cost is charged in accordance with the POW developed and agreed with the SSSB Board.

APP093 Enterprise Architect Application Service

Service ID: APP093

Service Name: Enterprise Architect Application Service

Service Type: Customer Facing

Portfolio Group: Application Services

Service Status: Pipeline

Service Description:

Service is based on the application Enterprise Architect (EA), which is a visual modelling and design tool based on UML. EA supports:

- the design and construction of software systems;
- modelling business processes;
- modelling industry based domains.

It can be used not only to model the architecture of systems, but to process the implementation of these models across the full application development life-cycle.

Systems modelling using UML provides a basis for modelling all aspects of organizational architecture, along with the ability to provide a foundation for designing and implementing new systems or changing existing systems. The aspects that can be covered by this type of modelling range from laying out organizational or systems architectures, business process reengineering, business analysis, and service-oriented architectures and web modelling, through to application and database design and re-engineering, and development of embedded systems.

Value Proposition:

Provisioning of Enterprise Architect application as a service supports complete system/application lifecycle management, starting from requirements modelling down to physical components, artefacts and infrastructure, while enabling architects/designers/analysts and software developers to benefit from a complete traceability between each model. Out of the box, EA has support for industry leading standards for system analysis and design (Unified Modelling Language - UML), business process analysis (Business Process Modelling Notation – BPMN, Decision Modelling Notation – DMN) as well as enterprise architecture modelling (ArchiMate 3.0.1, TOGAF). Many other standards are supported out of the box (ArcGIS,Iconix, SoMF, SysML and others).

Enterprise Architect supports architecture development using NATO Architecture Framework (NAF v4), with a free MDG plugin for Enterprise Architect. It also includes document templates for Business Analysts (based on Business Analysis Body of Knowledge – BABOK), Business Architects (based on Business Architects Guild’s BIZBOK). Additionally, it includes design-to-code with code generation from model, and data base entities generation from the model.

Service Flavours and Features:

1. Enterprise Architect – provision of a validated standalone software deployable on authorized networks, enabled for a single user, without collaboration features like

access to a shared network database repository. It is installed directly on an end-user terminal;

2. Collaboration Repository – provision of a collaboration repository, hosted on central infrastructure, enabled for an access to a shared network database repository, requires holding a valid Enterprise Architect (Flavour 1). This option enables true collaboration for a team of experts, knowledge sharing and exchange, discussions and shared project planning/execution.

3. ProCloud and Prolaborate Integrations - Prolaborate allows users to create tailored set of views that reduce complexity, focus attention and increase the accessibility of model information for the non-modelling community who are more concerned with consuming the models. Prolaborate also provides dashboards, impact analysis, gated reviews and much more to leverage information from the model to provide unique windows into the model for a custom audience.

4. Training package

Activities in scope of service:

- Service management of entire service lifecycle including regular user communication;
- Requirements analysis and validation with the customer:
    - Propose technical solution;
    - Evaluate and propose costs based on requirements and technical solution;
- Application management:
    - Incident Management:
        - Issue Investigation and Resolution; Escalation of tickets to 3rd party supplier when required and follow up until their final resolution;
    - Independent Verification & Validation:
        - Change Configuration Proposal (CCP) Submission and Follow up;
    - Deployment:
        - Configuration & Reconfiguration;
        - Deploying & Release, and Patches Management;
    - Operations:
        - Operate and perform the required maintenance on the application servers and the underlying platform;
        - Set up and Maintenance required Reference/Test and Development environment in NSF and make it available for the customer.

Available on:

- NATO Unclassified
- NATO Restricted
- NATO Secret
- Mission Secret

The service may be available, on request, on other security domains.

Service Prerequisites:

- WPS001 Managed Device Service
- WPS002 User Access Services

Standard Service Support Levels*:* N/A

Service Availability Target: 99.5% Yearly Availability for flavour 2 and 3, which have backend services

Service Restoration: For collaborative versions using repository only – service restoration within SLA boundaries.

Service Cost / Price: The cost is calculated per Flavour per number of users, number of repositories (costing model still under development, to request this service a CRF is required in order to obtain a price proposal).

APP095 Agile Tools for task management - JIRA Software Service

Service ID: APP095

Service Name: Agile Tools for task management - JIRA Software Service

Service Type: Customer Facing

Portfolio Group: Application Service

Service Status: Pipeline

Service Description:

JIRA is a family of software products that various types of teams can use to manage issues and tasks and handle daily team work, activities and objectives.

JIRA Software (JS) is the product based on Agile methodology that can be used for planning, tracking and reporting internal team activities. Teams and team managers can use the included boards for task management based on Agile methodology. Additionally Jira Software can be used for task management, software development, software testing, bug tracking, Agile project management, scrum management. Team productivity can be monitored using the included time tracking capabilities. Real time reports on progress are available.

JIRA Service Management (JSM) is the product used for ticket and request management that enable teams of agents to be in contact with customers and solve various non-it, business types of requests. Jira Service Management provides any service team the capabilities to be in contact with the customer and answer customer's requests according with procedures and SLAs in place. Team productivity can be monitored using the included KPIs and time tracking capabilities. Real time reports on status progress are available.

Confluence is the knowledge base product that can be integrated with both Jira Software and Jira Service Management. It can be used:

- with JIRA Software, to improve the documentation and information available to team members;
- with JIRA Service Management, to provide a self-service place to find answers before asking questions.

Value Proposition:

The service offers customer:

- by using JS accessing Scrum and Kanban boards out-of-the box (boards are task management hubs, where tasks are mapped to customizable workflows);
- by using JS, boards provide transparency across teamwork and visibility into the status of every work item;
- by using JS, boards can be used as activity lists for the team or team members;
- by using JSM tracking of activities inside teams if a process requires multiple team members to interact or it takes a long time to complete;

- by using JSM the possibility for a customer of a service team to make non-it requests to that service team and track request status until is resolved (requests are mapped to customizable workflows);
- by using Confluence, a knowledge base can be built and it can contain information related to processes, procedures, workflows, documents;
- by using Confluence integrated with JSM a knowledge portal with most common problems, procedures and solutions can be implemented;
- by using Confluence integrated with JS the activities and tasks inside JS can be documented;
- team productivity can be monitored using the included KPIs (for JSM), time tracking capabilities (for both JS and JSM) and real time performance reports with sprint reports and velocity charts (for JS).

Service Flavours and Features: Service is available as one of the 3 flavours below and in each case this consists of the base software and the add-ons as listed for each of the base software. Flavours can also be combined, depending on the request.

1. JIRA Software, including the add-ons:
    - Zephyr Scale – Test Management for JIRA Data Center
    - Configuration Manager for Jira (CMJ) Data Center
    - R4J – Requirements Management for Jira Data Center
    - Xporter – Export issues from Jira Data Center
2. JIRA Service Management, including the add-ons:
    - Kanban Boards for Jira Service Management
    - Refined for Jira
3. Confluence - Can be used as a standalone deployment or integrated with JIRA Software or JIRA Service Management;
4. Training

Activities in scope of service:

- Service management of entire service lifecycle including regular user communication;
- Requirements analysis and validation with the customer:
    - Propose technical solution;
    - Evaluate and propose costs based on requirements and technical solution;
- Application management:
    - Incident Management:
        - Issue Investigation and Resolution; Escalation of tickets to 3rd party supplier when required and follow up until their final resolution;
    - Independent Verification & Validation:
        - Change Configuration Proposal (CCP) Submission and Follow up;
    - Deployment:
        - Configuration & Reconfiguration;
        - Deploying & Release, and Patches Management;
    - Operations:
        - Operate and perform the required maintenance on the application servers and the underlying platform;

- Set up and Maintenance required Reference/Test and Development environment in NSF and make it available for the customer.

Available on:

- NATO Unclassified
- NATO Restricted
- NATO Secret

The service may be available, on request, on other security domains.

Service Prerequisites:

- WPS001 Managed Device Service
- WPS002 User Access Services

Standard Service Support Levels:

Service Availability Target: 99.5% Yearly Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period is 8 hours.
N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the relevant NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery (costing model still under development, to request this service a CRF is required in order to obtain a price proposal).

APP099 Data Science Software as a Service

Service ID: APP099

Service Name: Data Science Software as a Service

Portfolio Group: Data Science Application Services

Service Description: The Data Science Software as a Service (DS-SaaS) layer provides data science applications hosted in a protected and secure environment. The application can be exposed to users to test implementations and concepts but without endangering operational systems. This is not a full production environment, but is sufficient to host Minimum Viable Product (MVP) implementations of decision aids and other data science applications for extensive periods of time. This will allow the tools to be trialled in exercises and even in operations before going into full production.

DS-SaaS is hosted in on the DS-IaaS layer. For each application that is hosted in this DS-SaaS layer, NCIA provides subject matter expertise to support changes or issues.

Value proposition: The Service offers the following benefits:

- Improved decision speed and quality through application of artificial intelligence.
- Improved efficiency through automation of time-consuming tasks.

Service Features: Data Science Software as a Service offers the user the following features:

- Automated execution of specific functions, utilising AI-driven decision making.
- Increased effectiveness for data / document intensive functions e.g. analysts.

Service Flavours: Service flavours are result of combination of the following options:

- Series of Data Science & AI portal services

Available on:

NATO SECRET, classification up to including NS

Service Prerequisites:

WPS001 for NS services.

Service Availability Target : 98%

Service Restoration Priority : P3

N.B. This service is not intended to support operational or business users directly.

Service Cost / Price: The unit of measure for the *S*ervice flavours is per unit. Initial fee for subscribing to the service applies. There is an additional cost per named user of the portal(s), as well as an additional cost per named consumer of the portal(s); additional costs apply only one time if subscribing to multiple Data Science services hosted in SANDI. There are additional fees per named user depending on the user profile type (SaaS portal user profile or Consumer User profile).

Advanced Portal (PaaS) User Profile
User profile required for those working on virtual machines (IaaS or PaaS) on NATO SECRET Data Science Infrastructure.

Portal (SaaS) User Profile
User profile required for those developing on or publishing to portals on NATO SECRET Data Science Software as a Service (SANDI onpremises environment). This profile is only related to SaaS portals, and does grant access to virtual machines (IaaS or PaaS) on NATO SECRET Data Science Infrastructure as a Service (SANDI on-premises environment).

Portal (SaaS) Consumer Profile
Consumer profile required for those (re)viewing results published to portal on NATO SECRET Data Science Software as a Service (SANDI onpremises environment). This profile is mainly intended for stakeholders to projects, to allow early access to work under development.

Portal	Description	Unit
Dashboard Power BI SANDI Artificial Intelligence	Prepared Dynamic Dashboards	Per 1 unit: • 2 publishing users Unlimited (fair use) consumers
Analytics KNIME SANDI Artificial Intelligence	Self-Service Analytics Analytics as a Service (API)	Per 1 unit: • 2 publishing users • Shared processing hardware capacity Unlimited (fair use) consumers Option of adding dedicated hardware for processing (costs: DS-IaaS + labour)
jupyter Laboratory JUPYTER SANDI Artificial Intelligence	Data Exploration Model & Algorithm Experimentation	Per 1 unit: • 2 users • Shared processing hardware capacity Option of adding dedicated hardware for processing (costs: DS-IaaS + labour)

	Project Support Source Repository	Per 1 unit: • 2 users • 100 GB storage
	Personal / Team On-premises Cloud Storage Datasets	Per 1 unit: • 2 users • 100 GB storage Additional storage capacity can be requested
AI Pipeline Solutions NLP Natural language processing Natural Language SANDI Artificial Intelligence	Hosted Large Language Models (OpenAI OpenAPI chat compliant) Chat User Interface	Per 1 unit: • 1 million tokens (± 200,000 words) On-premises hosted models that can be used in combination with classified data up to including NS

APP100 Mobile Advisor Reporting Tool (MART)

Service ID: APP100

Service Name: Mobile Advisor Reporting Tool (MART)

Service Type: Customer Facing

Portfolio Group: Application Services

Service Status: Available

Service Description: The Mobile Advisor Reporting Tool (MART) enables Civil-Military Cooperation (CIMIC) / J9 staff to capture and record the outcomes of their engagements in the field. Through a modern, simple and user-friendly Internet accessible web application, end-users can draft, save and submit their engagement reports that will be delivered to the Advisor Network (ANET) database. Reports can be sent over data diodes, so they can reach the high side HQ operational network, not connected to the Internet.

Value Proposition: Accessible via any mobile device, this cloud-based application provides end-users with the capability of submitting engagement reports from anywhere and right after the engagement has taken place. Once the reports are processed and stored in the ANET database, they are deleted from the cloud storage to ensure confidentiality of the collected information.

Service Features:
MART comprises the following features:

- Draft, save, print, export (as PDF), and submit engagement reports
- Cloud-based front-end application reachable from any internet enabled Mobile Device
- Tailored report template including lookup tables and free-text fields
- Storing of submitted reports in the Advisor Network database
- Report Attachments
- Supports for external authentication services, such as, but not limited to, AWS Cognito, OpenID Connect, SAML, Active Directory Federation Services

Service Ordering and Request: Customer Request Form

Service Flavours: The Service is available in 3 flavours, based on the number of users:

1. Small deployment: 0-200 users
2. Medium deployment: 200-2,000 users
3. Large deployment: 2,000-10,000 users

Available on: Public accessible Internet services, limited to NATO UNCLASSIFIED content

Service Prerequisites:

APP068 – Advisor Network Application Service

Standard Service Support Levels*:*

Service Availability[1] **Target:** 99.0% Availability

Service Restoration:

Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Reporting: Standardised service reporting to customers in accordance with the NCI Agency SLAs

Available NCI Academy Training not covered by service cost: N/A

Service Cost / Price: The unit of measure for the service is Per Deployment. Price details available in the Service Rates Document.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP102 – REACT – PNT and NAVWAR Application Service

Service ID: APP102

Service Name: REACT – PNT and NAVWAR Application Service

Portfolio Group: Application Services

Service Description: The REACT – Positioning Navigation and Timing and Navigation Warfare Application Service is based on the Navigation Warfare functionalities of the NATO Software REACT (Radar, Electronic warfare and Communications coverage Tool). It provides the operational user with an intuitive way to develop Navigation Warfare (NAVWAR) products allowing decision makers to increase their situational awareness during planning and execution of air, ground or maritime operations. The operational user can generate predictions of Global Navigation Satellite System (GNSS) jamming effects within an area of interest based on specific GNSS jammer parameters and propagation models. The REACT tool can be hosted within the NATO Command Structure's Bi-Strategic Command (Bi-SC) Automated Information System (AIS) or hosted on a standalone local instance or internet-facing computer.

Value Proposition: REACT provides the NATO Navigation, Electromagnetic Operations Warfare and Space Communities with a capability that enables the following operational benefits:

- Support the Intelligence and other relevant Communities in visualising and understanding the effects of collected data from NAVWAR jamming systems.
- Sharing of intelligence services and data across NATO at all command levels.
- Enhance the dissemination of intelligence with Nations and other domains.
- Increased support to situational awareness, common operational picture, and mission planning and execution.
- Support to all operational mission types.
- Unique analytics and propagation modelling capability not available in other NATO systems.
- Support exercises and training activities within the NAVWAR, EMO and Space Communities.

Service Features: The REACT – PNT and NAVWAR Application Service is comprised of the following modules and features:

  - Front-end: a user-friendly Web application with services interacting with the REACT Tool back-end server modules
  - Back-end: a calculation module comprising of several advanced analytical models that returns results to the REACT Web client or other NATO FAS clients using the WMS data exchange format.

Service Flavours: The service is available as a single flavour.

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret

NATO Partner network (For NNHQ)

Service prerequisites:

APP055 - Core GIS Geospatial Services (pre-required if no WMS compatible mapping provision service is available)

Standard Service support levels:

Service Availability[1] Target: 99.5% Availability

Service Restoration: for NCS customers, the restoration priority will be as specified in centralised or local service level agreement.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP103 Business Process Management Application Service (BPM)

Service ID: APP103

Service Name: Business Process Management Application Service (BPM)

Portfolio Group: Application Services

Service Description: The Service enables organizations to model, analyse, measure, improve, optimize and automate business processes, though the use of workflows (a series of tasks or actions that are performed in a sequential/parallel manner to achieve an end goal, across different departments and physical locations).

Value proposition: A business process coordinates people, systems, information and things (IoT) to produce business outcomes in support of a business strategy. Business Process Management (BPM) is a valuable automation tool to generate a competitive advantage through cost reduction, process excellence, and continuous process improvement.

Service Features: The Service offers the following core functionalities:

- Graphical business processes modelling
- Business rules modelling
- Role-based access control
- Forms designer
- Process execution engine
- State management engine and reporting
- Ability to integrate with 3rd party tools.

Service Flavours: The service is available as a single flavour.

Available on:

NATO Unclassified
NATO Restricted
NATO Secret
Mission Secret
NATO Partner Network (For NNHQ)

Service Prerequisites:

WPS002 Enterprise Identity Access Management Service
WPS003 Enterprise User License Service
PLT003 Web Hosting Service

Standard Service Support Levels:

Service Availability Target: 99%

Service Restoration Priority: P2.

The Standard Service support comprises the following activities:

- **Operation**: application monitoring, log management, batch jobs management, backup & restore, auditing, Service Requests fulfilment.
- **Corrective Maintenance**: diagnosis and removal of the causes and the effects of any malfunction affecting the Service.
- **Preventive Maintenance**: preventive actions needed to avoid future malfunctions.
- **Adaptive Maintenance**: adjustment of the Service in order to adapt to the minor changes of the sub system components (i.e. Operating System, Database Management System, Browser, SharePoint and SharePoint add-ons). Major changes of the sub system components shall be requested via dedicated projects.
- **Minor Perfective Maintenance**: development of up to one minor workflow[1] per month[2].

Available NCI Academy Training not covered by service cost: No Academy Training available.

Service Cost / Price: The unit of measure for the Service is “per user”. Since the Service is designed for the general use by all the users of each customer, the number of user will be assumed to be equal to the sum of the “NATO Peacetime Establishment (PE)” users plus the “NATO Non-Peacetime Establishment (NPE)” users.

The cost of the Service does not include the cost of all the underlying Service prerequisites.

Each instance of the Service should be counted separately (so for example, if the same user is using two different instances of the Service on two different networks, the user should be counted twice).

The total amount of the Service delivery price is charged in accordance with specifically arranged conditions of the Service delivery.

[1] A “minor workflow” is defined as a workflow that requires in total not more than 5 man days in order to be designed, developed and tested.

[2] This activity will be paused during major implementation projects affecting the Service.

APP104 Medical Management Application Service

Service ID: APP104

Service Name: Medical Management Application Service

Service Type: Customer Facing

Portfolio Group: Application Service

Service Status: Available

Service Description: Medical Management Application Service facilities theatre medical staff in conducting Patient Tracking, Patient Regulating, Medical Capability Directory and Medical Reporting functions. The Medical Management application Service also enables the applicable contribution to Recognized Medical Picture to support Commander's decision making process.

Value Proposition: The Medical Management Application Service save lives through rapid decision making; medical management information is digitized empowering staff to make timely decisions based upon current situation information.

Service Features: The Medical Management Application Service provides minimum military functionality for the following medical functions: - Medical Capability Directory - Patient Tracking - Patient Regulating - Medical Reporting - Recognized Medical Picture. It can interoperate with Electronic Health Record capabilities and other medical capabilities to exchange information about the location and status of patients, medical capabilities, and medical missions.

Service Request: CRF can be raised for new request.

Service Flavours: Single flavour. Server based application with Web Client and a PostgreSQL Database Server

Available on:

NATO Unclassified
NATO Secret
Mission Secret

Service Prerequisites: WPS001 Managed Device Service

Standard Service Support Levels*:*

Service Availability[1] Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

APP107 NATO Unclassified Artificial Intelligence ChatBot

Service ID: APP107

Service Name: NATO Unclassified Artificial Intelligence ChatBot

Portfolio Group: Application Services

Service Description: The NATO Unclassified Artificial Intelligence ChatBot service is an advanced AI powered ChatBot for NATO Unclassified use. This service leverages the state-of-the-art artificial intelligence ChatGPT from Open AI, to deliver timely and informative responses to inquiries. The service adheres to NATO security requirements, allowing use for NATO activities up to NU. In addition, the commercial ChatGPT service can be augmented by extensive databases tailored to NATO's unique requirements and operational contexts. The service is accessible exclusively from NATO end user devices, ensuring confidentiality and integrity of inputs to, and outputs from, the AI service. This service is within the scope of the enterprise directive on use of generative AI.

Value Proposition: The NU Artificial Intelligence ChatBot service offers a unique value proposition by enhancing the speed and efficiency of a variety of text-based activities through instant access to vast repositories of information and effective text generation and summarisation functions. This service directly supports critical business processes by:

- **Reducing Information Retrieval Times:** Offering instant responses to queries, thereby accelerating the decision-making process and enhancing business efficiency.
- **Provide additional text processing capabilities:** offers assistance with document generation, summarisation, translation etc.
- **Improving Information Accuracy:** Leveraging curated databases and NATO-specific knowledge to provide accurate and contextually relevant information[1].
- **Enhancing Security:** Ensuring all interactions with AI are conducted through NATO's secure networks, maintaining the confidentiality and integrity of information.

By providing this service from NATO devices, it enables NATO personnel to achieve their objectives in less time, with greater precision and effectiveness, directly contributing to the success and efficiency of NATO business functions.

Service Features: The NATO Unclassified Artificial Intelligence ChatBot application is hosted on the Production Cloud and offers the following service features:

1. NATO-Specific Knowledge Base: The ChatBot is augmented with NATO Unclassified data with information relevant to NATO operations, policies, and procedures, ensuring responses are both accurate and applicable (pending NOS approval)[2]

[1] NOS needs to approve the usage of NU data to augment the responses of the AI ChatBot with relevant NATO information. In case that this approval is not provided, the AI ChatBot will be available in its vanilla form, where up to NATO Unclassified can be entered by the user in the question

[2] NOS needs to approve the usage of NU data to augment the responses of the AI ChatBot with relevant NATO information. In case that this approval is not provided, the AI ChatBot will be available in its vanilla form, where up to NATO Unclassified can be entered by the user in the question

2. Secure Interface: Designed to be accessed via NATO's secure networks, the ChatBot ensures that all data exchanges maintain the highest levels of security, in compliance with NATO's stringent cybersecurity protocols.

3. Multi-Lingual Support: Recognizing the diverse linguistic background of NATO personnel, the ChatBot is equipped to understand and respond in multiple languages, facilitating clearer communication.

4. High Availability: The AI ChatBot is available around the clock, providing uninterrupted access to information and functions whenever it's needed.

5. User-Friendly Interface: Designed with the user in mind, the ChatBot features an intuitive interface that requires minimal training, ensuring it is accessible to all personnel, regardless of their technical proficiency.

By offering these features, the NATO-Aware AI ChatBot is a pivotal tool in the arsenal of NATO personnel, designed to streamline business functions, improve staff efficiency operations and enhance the effectiveness of the enterprise.

Service Flavours:
The service comes with two flavours:

- AI Basic, offers secure access and includes usage of GPT-3.5 (the default ChatGPT model)
- AI Advanced: add-on on top of AI basic flavour, that can be purchased by an organisational unit, offering a higher performing AI model (GPT-4).

Available on:
NATO Unclassified

Service Prerequisites:
PLT010 Production Cloud

Service Availability Target: 99.5% Availability

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is 4 hours on working days.

Service Cost / Price: The unit of measure for the Service is "per user".

APP108 NATO Maritime Availability Database (NMAD) Service

Service ID: APP108

Service Name: NMAD Application Service

Service Type: Customer Facing

Portfolio Group: Application Services

Service Status: Available

Service Description: The NATO Maritime Availability Database (NMAD) Application Service provides an accurate and intuitive solution that enable Allied Maritime Command to visualise forthcoming presents of units in within SACEUR AOR, and associated forms of their support. Availability and readiness reports from all Allied NATO maritime assets has been requested to confirm future unit position, intended movement, readiness and availability. A critical element of this is to understand on a continuous basis the availability of maritime units at sea and to manage continuous availability and readiness for National maritime units for potential NATO tasking.

Value Proposition: The service is integral to the Maritime Community of Interest and offers the following benefits:

- Provides command awareness of maritime friendly units, which could be made available for NATO tasking in the event of a crisis.
- Ensures 360 degrees maritime focussed awareness and connectivity
- Utilizes historic information for campaign assessment, operational evaluation and retrieval.
- Receives information about the future presence of units in defined areas and their form of support.
- Automatically reads the national messages, stores them and generates the required reports and dashboards.
- Supports the operational user in managing the messages by allowing message data updates.
- Enforces a standard format for the messages.
- Presents data in a structured format.

Service Features: The NMAD Application Service is comprised of the following applications:

- NMAD – Web based tool – for Planning/Scheduling and Commander Situation Awareness

Service Ordering and Request: The new service instances are requested and created by submitting standardised service requests (work orders) through the ITSM toolset; for customers there is no specific service initiation cost associated with NMAD Application Service.

Service Flavours: NMAD Application Service may be fully customised to meet requirements of a specific customer or a specific site.

Available on: NATO Secret

Service Prerequisites:

WPS001 Managed Device Service

APP055 Core GIS Geospatial Services

APP007 Tools for Operations Planning Functional Services (TOPFAS) Application Service

Standard Service Support Levels*:*

Service Availability[1] Target: 95%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident is 4 hours. Availability of the “NMAD application service” is primarily dictated by the availability of the underlying Managed Devices Service.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Reporting: ACO/ACT Customers: The standardised service reporting is provided as a deliverable of this service. ACO standardised reporting templates are listed in the SLA Annex 18 and managed by ACO KPI/KQI WG.

Quarterly Reports:

Service availability and service performance reports at Service Access Point (SAP) (via incidents) Incident management report base on ITSM tickets and trend analysis Change management and ASI report based on ITSM tickets Asset and Configuration Management report.

Additional service reporting requirements can be requested through the respective SLAs it may be

subject to additional service fees.

Available NCI Academy Training not covered by service cost: There is no training offered by the NCI Academy

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum “Monthly Uptime Percentage” for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

APP110 Information Environment Assessment (IEA)

Service Name: Information Environment Assessment

Service Type: Customer Facing

Portfolio Group: Application Service

Service Status: Pipeline

Service Description: The IEA service provides to NATO consumers of Publicly Available Information (PAI) an integrated data-sourcing and analytics platform to collect and understand the Information Environment (IE).

Value Proposition: The IEA service provides the following value and benefits:

- Consolidated data access: the IEA service provides a hub for PAI, aggregating data collected through commercial subscriptions, Internet scraping, audience research, and ad-hoc PAI sources. The IEA service allows the data to be filtered to focus on NATO's topics of interest.
- Advanced data analytics: the IEA services leverages the latest data analytics methods, generative AI, entity extraction to expose data to the NATO analyst in the form of interactive dashboards and visualizations to support collection and data exploitation.
- System environment: the IEA service provides a NATO-hosted collaborative environment allowing the PAI-consuming operators to organize and plan their collections, create and store bundles of processed data for archival, further retrieval and processing, and use advanced hosted analytics on NATO internal data.

Service Features:

- Commercial subscriptions: provides the ability to connect to existing data sources, or to trigger the procurement of additional ones to meet domain-specific requirements.
- Internet scrapers: provides the ability to collect specific data directly on the surface web, and selected areas of the deep web and dark web.
- Data-science and collaboration platform: provides the ability to search, transform, share and present data.
- Data-science support: provides the ability to get data-science and AI subject matter experts integrate ad-hoc data sources, develop advanced visualizations or provide consultancy on to PAI communities of interest.

Service Request:

- Access to the IEA service based on existing service features (data-sources, analytics) will be requested through ITSM service requests on a per-user account basis.
- Requests for additional service features will be managed through a data change process, in order to capture community-specific requirements, the procurement strategy, and funding.

Service Flavours:

1. IEA system environment management: the NCIA service delivery manager will provide the 2nd level support to the IEA platform, manage service requests and incidents, and collect continued improvement feedback and data requirements.
2. IEA data-services contracts management: the NCIA contracting officer and the NCIA service delivery manager acting at the Contracting Officer Technical Representative (COTR) will manage the performance of the existing data-services contracts and validate the service level agreement metrics.
3. IEA data-services contracting: the NCIA contracting officer and the NCIA service area owner will organize the procurement of additional data services or the renewal of the existing ones, based on the NATO acquisition procurement regulations. This process can have a variable time range depending on the magnitude and complexity of the services requirements.
4. IEA data-science support: the NCIA data-scientist and operational analyst will support the service users to optimize the use of their data, incorporate ad-hoc data-sources and analytics into the IEA platform, support recruitment and training of analysts in the NATO Enterprise.

Available on:

- NATO UNCLASSIFIED
- NATO-operated Azure public cloud & commercial Internet platforms

Service Prerequisites:

- The IEA service users will need Microsoft Online accounts to access the IEA system environment.
- The IEA service users will need contractor-specific accounts to access the IEA analytics platform.
- The IEA service users can optionally subscribe to the Enterprise Internet Service [INF003], service flavor Anonymized Browsing, in order to meet the non-attributable identity requirements for the service.
- The IEA platform requires the Cloud Services Management and Integration (CSMI) Service [PLT010] for the hosting, security and operations of the IEA platform.

Standard Service Support Levels:

Service Availability[1] Target: the service availability target is negotiated on a per-data-service basis. The target for the data-services contract is 98% during business hours (Mon-Fri 08.00-18.00 CET), meaning a maximum of 1 hour downtime per week on a quarterly average.

Service Restoration: the service restoration target is 2h during business hours (Mon-Fri 08.00-18.00 CET) and 12h outside business hours.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

Security Services

This page is left blank intentionally

SEC001 Security Accreditation Support Service

Service ID: SEC001

Service Name: Security Accreditation Support Service

Portfolio Group: Security Services

Service Description: The Security Accreditation Support Service provides guidance and support for security accreditation and re-accreditation activities for active and pipeline services, including the preparation of documentation required to support Security Accreditation.

This service only includes the Agency's centralised resources required for delivery. Local support from collocated staff in support of day-to-day operations is not included and must be funded locally.

Value Proposition: Support to Cyber Security - Assessment. This service enables the reduction of security risk to the NCI Agency, ensuring Cyber Security Policies, Architectures and Acquisition strategies, internally and externally, are coherent and effective. Additionally it provides assurance and stability of a well understood regulatory framework by all stakeholders.

Service Features: Security Accreditation Support Service is comprised of the following elements:

> **Security Accreditation Preparation and Documentation (New Systems):** Development of Security Accreditation Plan (SAP) together with project manager and obtaining approval to proceed from relevant Security Accreditation Authority (SAA). Working together with project team on development of security accreditation package (usually CIS description, Security Risk Assessment, Security Requirement Statement, Security Operating Procedures and Security Test and Verification Plan and Security and Verification Test Report) for new systems. Providing guidance and assistant to project team. Review of security accreditation package developed by project team. Coordination with relevant NATO Security Accreditation Authorities during project life cycle. Serves as first Point-of-Contact for Accreditation of new systems. This service feature is only available to and funded by projects that deliver new CIS that require accreditation.
>
> **Security Accreditation Support (In-service systems):** Provision of cyber security technical and policy support to Operational Commands and CIS Operating Authorities to manage risks and assist in the continued security accreditation of their CIS. Working together with System Managers and CIS Security Officers on updating of security accreditation package (usually CIS description, Security Risk Assessment, Security Requirement Statement, Security Operating Procedures and Security Test and Verification Plan and Security and Verification Test Report) for re-accreditation of systems in service. Providing guidance and assistant to System Managers and their team. Review of security accreditation package during CIS re-accreditation process. Comprehensive coordination with the NATO CIS Security Accreditation Board (NSAB) or any applicable Security Accreditation Authority (SAA). Guidance and support on security accreditation and re-accreditation activities as required by the NATO SAA's.

Support for development of security accreditation strategies. Serves as first Point of Contact for re-accreditation of in-service systems.

CIS Security Conformity Support: Support towards formal attestation (e.g. in form of Electronic Security Conformance Statement (ESECS) for DCIS) that the prescribed security measures from CIS-specific security accreditation package are in place. This ensure that new or modified CIS meet the security expectations of the customer as well as the requirements of the NATO Security policy and supporting directives before being deployed and activated.

Coordination in Security Risk Assessment Working Groups: Support, lead, or coordinate Security Risk Assessment Working Groups for NATO programmes or projects. This includes lead or coordinating the meetings and ex-committee work, providing advice regarding security risk assessment and risk management process, and support conducting SRA by the Group. Specifically for the NATO Security Risk Assessment Group (NSRAG) this services entails the review and approval (in coordination with SAAs) of the specification of risk assessment/management tools used for NATO CIS (e.g. NATO profile for PILAR), the development and maintenance of generic security risk assessment for NATO CIS scenarios as well as support of NOS and the Security Committee in CIS Security format in the review / development of NATO documents addressing security risk assessment / management and provision of support to NSAB.

Support for Board of CIS Operational Authorities (BCISOA): in 2022 NCI Agency NCSC Accreditation Support Office became an augmented member of BCISOA (Ref. OCIO(2022)0147 dated 13/12/2022). This service feature includes participation and contribution to BCISOA meetings, conducting relevant actions from these meetings and ex-committee coordination with BCISOA members.

Service Flavours: The Service is available in the following flavours:

- **Security Accreditation Preparation and Documentation (New Systems):** As described in the Service Feature. This flavour must be funded by each project that is seeking to achieve accreditation.

- **Security Accreditation Support (In-service systems):** As described in the Service Feature.

Service Available on:
Network neutral

Service Prerequisites: Validation of operational requirement for new CIS and extension of CIS in service.

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery for In-service Systems.

SEC004 Cyber Security Analysis Service

Service ID: SEC004

Service Name: Cyber Security Analysis Service

Portfolio Group: Security Services

Service Description: Cyber Security Analysis Service is responsible for collecting and analysing digital evidence and threats (malware code) using a variety of specialized tools and techniques and a wide-variety of data sources and physical and virtual assets. The service is a cornerstone to support efficient Incident response, as well as to help fine-tuning detection and leverage expansion actions and threat hunting campaigns. The service provides technical analysis outcome and artefact for further Cyber threat assessment and for sharing with the NATO bodies, NATO nations and the other NATO partners within the agreed frameworks. The service also support the mitigation, remediation and post-incident phases.

This service only includes the Agency's centralised resources required for delivery. Local support from collocated staff in support of day-to-day operations is not included and must be funded locally.

Value Proposition: Support to Cyber Security - Defence. This service provides greater insight into potential security threats that contribute to lowering business risks. Furthermore informing better future prevention strategies obtained through a deep understanding of the nature of malware and forensic analysis.

Service Features: Cyber Security Analysis Service is comprised of the four following elements:

- **Forensic Analysis:** Performs online (OCF) and stand-alone (SCF) computer forensics analysis for Incident Management and on-request for specific use case.
- **Malware Analysis:** Carry out technical analysis on suspicious application code to identify any malicious content. Sharing of technical characteristics of malware within a trusted community either on an *adhoc* basis or via an automated MISP platform.
- **Evidence Acquisition:** Acquires in a forensically sound manner a variety of data source, physical or virtual assets for further processing by authorised NATO bodies.
- **Compromise Assessment[1]:** Provision of resources during or post incident analysis to validate that a customer's systems and/or information (i.e. document set, database content) are free of malware.

Service Flavours: The Service is available as a single flavour.

Service Available on:

NATO Unclassified
NATO Restricted

[1] Compromise Assessment is currently limited to those customers who may require this service feature as part of incident response. Specific requests from customers to confirm "clean" data received from third-parties is considered a new requirement and is not supported. Surge capacity for this service feature, via support from industry, is currently not funded.

NATO Secret
NATO Mission networks (not C-SLA funded)

Service Prerequisites:

Analysis activities require the provision of resources to ensure that all NCSC Operational Applications are maintained to ensure they meet optimal performance, can include but not limited to, sensor tuning, signature updates, application updates, performance tuning, forensics agents deployment and connectivity to NS, NR, NU, MS.

SEC029 delivers the PaaS to host SEC004.

Mandatory Dependencies:

SEC006 Cyber Security Incident Management Service

SEC007: Cyber Security Monitoring – perform network and log analysis

SEC008: Cyber Security OPCEN – coordination and 24/7 availability

SEC010: Cyber Security Information Sharing – sharing of cyber threat intelligence to NATO and NATO nations

Standard Service Support Levels:

Support Hours: Cyber Security Analysis service is available 24/7, 365 days per year, aligned w/ NCIA business hours for on-site support (Mon-Thu 08.30-17.30, Fri 08.30-15.30), The service is available outside of business hours including weekends/holidays via Cyber Security OPCEN (NCN 626 6666, see service SEC008). During these outside hours, the on-call support includes the recall of on-call staff in the office on decision of the On-call SEC006 Cyber Incident Responder.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC005 NATO Cyber Defence Rapid Reaction Team/Security Response Team

Service ID: SEC005

Service Name: NATO Cyber Defence Rapid Reaction Team/Security Response Team

Service Type: Customer Facing Service

Portfolio Group: Security Services

Service Description: Provides rapid, technical cyber defence assistance to NATO organisations (Security Response Team (SRT)[1]) and to individual NATO Allies subject to Council decision on a case by case basis (NATO Cyber Defence Rapid Reaction Team (RRT)). The RRT/SRT's foundation is the provision of 2 x teams of NATO cyber experts but it can reach into NCI Agency's staff for deep expertise in order to deploy capabilities similar to those of the NCSC, but at remote locations and in response to Cyber Security incidents and crises.

This service only includes the Agency's centralised resources required for delivery. Local support from collocated staff in support of day-to-day operations, or industry support, is not included and must be funded locally/separately.

Value Proposition: Support to Cyber Security – Defence. The Cyber Defence RRT/SRT provides flexible, deployable Cyber Security response where in times of crisis.

Service Features: The NATO Cyber Defence RRT/SRT is comprised of the following elements:

- Digital Forensics
- Malware Analysis
- Event/security Log collection
- Intrusion Detection System
- Full Packet Capture
- Online Vulnerability Assessment
- Incident Management

Service Flavours:

Deployed
Distributed
Centralized NCSC response

Service Available on:

NATO Unclassified

[1] The deployment of a RRT team to support a NATO organisation during an incident response is referred to as the Security Response Team (SRT) and is subject to Chief NCSC or NCIA GM decision that on-site support is warranted in order to provide the required timely response to properly triage the incident. The deployment of a RRT team to support a NATO ally is referred to as the Rapid Response Team (RRT) and is subject to Council decision on a case-by-case basis.

NATO Restricted
NATO Secret
NATO AOM networks

NATO nations networks (on a Council-approved, case-by-case basis)

Service Prerequisites: N/A

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC006 Cyber Security Incident Management Service

Service ID: SEC006

Service Name: Cyber Security Incident Management Service

Portfolio Group: Security Services

Service Description: Cyber Security Incident Management Service delivers cyber incident response according the NATO Office of the CIO (OCIO) Cyber Incident Response Plan (CIRP). The service aims at delivering an efficient and effective response for containing, analysing and removing the threat, coordinating the restoration of the affected services within NCSC, NCIA and the stakeholders in the various NATO bodies, NATO nations and the other NATO partners within the agreed frameworks.

This service only includes the Agency's centralised resources required for delivery. Local support from collocated Agency staff in support of day-to-day operations is not included and must be funded locally.

Value Proposition: Support to Cyber Security – Defence. This service provides a centralised Incident Handling and Response. The experienced, effective and efficient management of identified incidents through Cyber Security Incident Management Service ensure correct handling through incident lifecycle, in turn strengthening cyber security capability and therefore the overall effectiveness and productivity of the organisation.

The service is supported by the Cyber Operations Management System (COMS), implementing the Incident Management processes in accordance with the CIRP as well as providing a supporting platform for Information and Knowledge Management (IKM), hosting all the Standard Operating Procedures and Instructions. COMS is available for all NATO stakeholders on NATO Secret, and to NCSC on the NATO Restricted. COMS is funded as part of SEC006.

Service Features: The service is composed of: Incident Triage; Containment Eradication;;; Alerting, Reporting, and Assisting with Recovery and Follow-up; The service also includes the management of and contribution to Cyber Incident Task Force (CITF).

Service Flavours: The Service is available as a single flavour.

Service Available on:

NATO Unclassified
NATO Restricted
NATO Secret
NATO Mission networks (Not C-SLA funded)

Service Prerequisites: On-Line and On-site support, including logistical, security, technical and political coordination.

Mandatory Services

SEC004:Cyber Security Analysis – perform forensic and malware analysis

SEC007: Cyber Security Monitoring – perform network and log analysis

SEC008: Cyber Security OPCEN – coordination and 24/7 availability

SEC010: Cyber Security Information Sharing – sharing of cyber threat intelligence to NATO and NATO nations.

SEC029: Cyber Security Platform and Infrastructure Service. Provide the infrastructure on which all mandatory supporting cyber security services (SEC004, SEC007. SEC008, SEC010) are running.

Standard Service support levels: N/A

Service Availability: 24/7

Maintenance Services: no set schedule

Support Hours: Cyber Security Incident Management service is available 24/7, 365 days per year, aligned w/ NCIA business hours for on-site support (Mon-Thu 08.30-17.30, Fri 08.30-15.30), The service is available outside of business hours including weekends/holidays via Cyber Security OPCEN (NCN 626 6666, see service SEC008). During these outside hours, the on-call support includes the recall of on-call staff in the office.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC007 Cyber Security Monitoring Service

Service ID: SEC007

Service Name: Cyber Security Monitoring Service

Service Type: Customer Facing Service

Portfolio Group: Security Services

Service Description: The Cyber Security Monitoring Service provides the monitoring of networks, websites and email traffic to detect and identify threats and compromises, and so to ensure cyber security.

This service only includes the Agency's centralised resources required for delivery. Local support from collocated staff in support of day-to-day operations is not included and must be funded locally.

Value Proposition: Support to Cyber Security – Defence. This service is designed to detect incidents – as a prerequisite to incident response. By monitoring hundreds of millions of events each day feeding a Security Incident and Event Management (SIEM) and processed by NCSC-maintained correlation rules, the Cyber Security Monitoring Service delivers cyber security of NATO CIS by providing assurance that:

- Email data spillages are detected and minimised
- Monitored website in question is available and undefaced
- Events will be correlated and scrutinised by qualified and experienced Security Analysts for appropriate actions as required

Service Features: This service is comprised of the following elements:

- **Internet Facing E-Mail Content Monitoring:** The provision of the ability to check all Inbound/Outbound Internet e-mail to ensure compliance with NATO and applicable local Security Polices; such checks include malicious code, executable content, encrypted content, SPAM, and Classified Data content. Outbound e-mail can be monitored either centrally by NCSC, or locally by appropriate IA Staff.
- **Internet Web Site Monitoring:** The ability to centrally monitor customer's Internet-facing Web Sites for unauthorised changes and to take appropriate reporting/remedial actions.
- **Network Monitoring:** Network Intrusion Monitoring, Detection & Prevention is the provision of centrally managed and monitored Network-based and Host-based technologies and feeds, for instance Network Intrusion Detection/Prevention systems, Application-aware firewalls, Web proxies and reverse-proxies, antimalware products, security and system logs, actionable threat intelligence, etc.

Service Flavours: The Service is available as a single flavour.

Service Available on:

NATO Unclassified

NATO Restricted
NATO Secret
NATO AOM Networks

Service Prerequisites:

SEC011 – Gateway Security Service
Provision of resources to ensure that all NCSC Operational Applications are installed and maintained to ensure they meet optimal performance, can include but not limited to, sensor tuning, signature updates, application updates, and performance tuning.

Provision outage and change notifications in order to minimise false-positives.

This service must be activated in conjunction with SEC006 (Incident Response), SEC004 (Technical Analysis) and SEC010 (Information Sharing). They are mandatory dependencies.

This service relies on the PaaS and SaaS delivered by SEC029, a mandatory dependency.

Standard Service Support Levels:

Service Availability Target: N/A

Service Restoration: 2 business days.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC008 Cyber Security OPCEN Helpdesk Service

Service ID: SEC008

Service Name: Cyber Security OPCEN Helpdesk Service

Service Type: Customer Facing Service

Portfolio Group: Security Services

Service Description: Cyber Security OPCEN Helpdesk Service provides the customers with a single point of contact for cyber security related incidents, requests and advice, as well as for cryptographic equipment configuration and keying. This service is a 24/7 provided service.

This service provides assurance that:

- cyber security incidents are reported to a single point of contact and correctly escalated;
- customers have a single point of contact to push requests or ask for advice from any NCSC organizational entity;
- crypto-related issues are reported to a single point of contact;
- customers experiencing crypto configuration issues are helped in applying the configuration changes needed to operate properly TCE crypto devices;
- NPKI certificate related requests (issue, revoke) are raised to a single point of contact.

Value Proposition: Support to Cyber Security – Defence. Continually accessible advice and action to support the customer in the maintenance of efficient and compliant cyber security and cryptography that underpins the security of our communication and information.

Service Features: This service is comprised of the following features:

1. SEC008/1: **24/7 single point of contact for cyber security related incidents, requests and advice:** 24/7 presence of specialists to give advice on potential cyber security incidents (and appropriate escalations as required) and 24/7 helpdesk for reporting the cyber security incidents (SEC006) and the ITIL incidents related to NCSC services. Cyber Security Incident management Service provides COMSEC and COMPUSEC, incident violation and insecurity investigation. The service enables an effective and efficient response to immediately contain a detected and/or reported incidents, including incident containment, eradication, recovery and follow-up.

2. SEC008/2: **24/7 helpdesk for IP Crypto devices:** Operation of IP Crypto Central Management System and 24/7 helpdesk to support cryptographic equipment issues, CRYPTO key changes coordination, verification and reporting, troubleshooting and ITIL Level 1 and 2 support.

3. SEC008/3: **24/7 support for cryptographic devices installations:** 24/7 support to new cryptographic devices installations or changes to existing infrastructure, including Production of user configuration data sheets and Creation of units into the IP Crypto Central Management System.

4. SEC008/4: **Creation and revocation of NATO PKI certificates:** Provides a 24/7 single point of contact for creation and revocation of NATO PKI certificates.

Service Flavours: The Service is available as a single flavour.

Service Available on:

All NATO networks for SEC008
NSV2 for SEC008
NNCCRS for SEC008
SIGINT COINS for SEC008
NRF MS for SEC008
NRF NS for SEC008

Service Prerequisites:

This service has the following dependencies

SEC006 - Incident Response
SEC014 - Crypto Management
SEC015 - Security Certificate (NPKI)

Standard Service Support Levels: 24/7

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC009 Cyber Security Outreach Service

Service ID: SEC009

Service Name: Cyber Security Outreach Service

Portfolio Group: Security Services

Service Description: Cyber Security Outreach Service:

- Supports outreach in order to support NCSC development and, where appropriate, broader NATO Cyber Security aims. Promotes liaison amongst the wider Cyber Community of Interest (COI), facilitates related visitation support, contributes to information sharing through outreach programmes, and provides assistance with comprehension of regular Cyber Security reporting. Outreach includes contribution to Cyber Sitreps, briefings, portals, workshops, and other reoccurring, information campaign events.
- Risk Communication and Identification: Assists in the identification of and informing of relevant stakeholders on risk associated with NCIA-provided CIS and the cyber technical options available for mission objective planning, general information sessions, and as part of cyber incident response

This service only includes the Agency's centralised resources required for delivery. Local support from collocated Agency staff in support of day-to-day operations is not included and must be funded locally.

Value Proposition: Support to Cyber Security – Inform. This service enables improved cooperation between Cyber security entities, better representation of cyber security domain and improved representation of Cyber security requirements and priorities. Risk Communication and Identification informs relevant stakeholders in understanding the cyber risk associated with using NATO CIS for mission planning purposes, general awareness sessions, and during cyber incident response.

Service Features: This service is comprised of the following features:

- **Cyber Security Outreach:** Supporting outreach in order to support NCSC development and, where appropriate, broader NATO Cyber Security aims. Encouraging liaison amongst NATO cyber stakeholders and information sharing through existing outreach programmes, assistance with the comprehension of regular Cyber Security reporting. Outreach, including contribution to stakeholder engagement, briefings, contribution to NATO Cyber Training, portals and other information campaign activities.
- **Risk Communication and Identification:** Assists in the identification of and informing to relevant stakeholders on the risks associated with NATO CIS for the cyber-related activities planned or currently being undertaken.

Service Flavours: This Service is available as a single offering.

Service Available on:

NATO Unclassified
NATO Restricted

NATO Secret
Mission Secret

Service Prerequisites:

None

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC010 Cyber Security Information Sharing Service

Service ID: SEC010

Service Name: Cyber Security Information Sharing Service

Portfolio Group: Security Services

Service Description: Cyber Security Information Sharing and Reporting is the communication of specific, timely and authoritative guidance.

This service only includes the Agency's centralised resources required for delivery. Local support from collocated staff in support of day-to-day operations is not included and must be funded locally.

Value Proposition: Support to Cyber Security – Inform. The sharing of timely and accurate information is essential to maintain the cyber security strength of the organisation, as a proven way forward to increase/maintain security posture. The service also include development of new features for MISP and CDSA as part of continuous service improvement (CSI).

Service Features:

- Offers different portals offering a web view and in some cases Application Programming Interfaces (API) to deliver relevant cyber information to the different communities of interest.

- Bulletins (including NIMBL), briefings, operational reporting, portals and other communications with Cyber Security communities of interest. Generation of reactive advisories to mitigate discovered vulnerabilities or to reduce the impact of newly emerged threats.

Service Flavours:

Cyber Defence Information Sharing: An extended service from the Malware Information Sharing Platform (MISP), covering Cyber Defence-relevant information (e.g. indicators of compromise, threat actors infrastructure and tactics, technics and prodedures(TTPs), vulnerabilities) and enabling sharing among NATO, Nations and industries

This flavour is provided as:

1. a Multinational MISP (MN MISP) supporting the MN MISP Smart Defence project, led under the governance of the MN MISP Smart Defence Steering Board on NATO Unclassified;
2. a Partners MISP to industries (having signed Industry Partnership Agreement - IPA) and other partners (i.e. CERT-EU) on NATO Unclassified;
3. an unclassified MISP (NCSC MISP) to NATO Cyber Security Community of Interest on NATO Unclassified;
4. a classified MISP (C MISP) to the NATO Cyber Security community of interest on NATO Secret.

Cyber Defence Situational Awareness (CDSA) – Delivers custom dashboards, incident filtering and overall Situational Awareness for ACO CyOC and other key Cyber stakeholders.

Cyber Threats Security feeds (CTSF) – procure, deliver and manage access to Cyber Threat Information from various vendors to the benefit of the NATO cyber security and intelligence stakeholders.

The NATO Information Assurance Product Catalogue (NIAPC) established under Directive AC/322-D(2019)0041-REV1, provides NATO nations, and NATO civil and military bodies with a catalogue of Information Assurance (IA) products, Protection Profiles and Packages that are in use or available for procurement to meet operational requirements.

Service Available on:

NATO Unclassified (MISP, NIAPC, CTSF)
NATO Restricted (CDSA)
NATO Secret (CDSA, MISP)

Service Prerequisites:

SEC004, SEC006, SEC027 and SEC007 are mandatory sources of information for CDSA
SEC004, SEC006 and SEC007 are mandatory sources of information for MISP therefore dependencies.

SEC007delivers the SaaS to host SEC010 (CDSA).

SEC029 delivers the PaaS to host SEC010 for CDSA ,MISP and NIAPC.

Standard Service Support Levels:

Service Availability Target for all MISP instances and NIAPC: 99.0%

Service Availability Target for all CDSA instances are aligned to SEC007 SaaS
The Service Availability target, Service Desk support and incident response are applicable during office hours (8x5).
Data synchronisation from NCSC MISP (NU) to C-MISP (NS) has a target of once per day.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC011 Gateway Security Service

Service ID: SEC011

Service Name: Gateway Security Service

Portfolio Group: Security Services

Service Description: Gateway Security Services provide a secure interconnection of different networks or network sections in order to protect an organization's key information.

Service is comprised principally of the following technical components: Data Diodes, Firewalls, Guard, Mailguard and VPN.

This service only includes the Agency's centralised resources required for delivery. Local support from collocated staff in support of day-to-day operations is not included and must be funded locally.

Value Proposition: Support to Cyber Security - Prevent. Expert and effective Gateway Security management is a fundamental cyber security requirement, preventing compromise and facilitating secure connectivity.

Service Features: This service is comprised of the following elements:

Common to all:

- Configuration Backup
- Disaster Recovery / Business Continuity Services / Service Restoration
- Log forwarding to archiving and/or forensic systems
- maintenance of system software (not XLG)
- 24x7 device health and availability monitoring
- Device troubleshooting
- Documentation
- CCP / AFPL process for software updates
- Provide 365 days on-call support for high incidents
- Annual test and review of BCP
- Development of SOP for repetitive activities (level 1, limited level 2)
- Education/training/familiarization of other teams
- Audit, accounting, authorization
- Incident management, troubleshooting

Gateway Security – Firewall Services:

- Support of physical, virtual and cloud-based firewalls
- Access to firewall configuration and near real-time logs
- Policy management (unlimited policy changes, following ITSM requests)
- Device management (bi-annual FW software update, weekly security content updates, emergency updates)
- VPN support (Site-to-Site, Client/SSL VPN)
- (limited) Network Access Control configuration for the Client VPN
- Access configuration for Client VPN

- Exercise adaptation / policy and configuration management (CSLA covered exercises)
- Firewall rule review and recertification, removal of unused/no longer required rules
- Reporting of allowed services / Provisioning of current rule set to SAA
- Security Incident Management support
- Application of the incident response activities (blocking hosts, disconnecting networks, NIMBLs)
- Development of custom application signatures
- testing/evaluation of new features and capabilities
- Post deployment network adaptations and expansion (SRTS)

Gateway Security – Mailguard Services:

- Adaptation of release markings
- Adaptation of email attachment types
- Patch installation
- Mailguard software upgrades
- Troubleshooting connectivity issues
- (limited) End-user support to identify mail rejection issues
- Testing/evaluation of new features and capabilities

Gateway Security – VPN Services:

- routing / tunnel configuration for NAFI and BMD-NAFI

Gateway Security – Guard Services:

- configuration of additional FAS flows
- adaptation of release markings

Gateway Security – Data Diode Services:

- configuration of new flows (SMB)
- configuration of new email domains

Gateway Security – IEG-C Services:

- configuration of new flows and access requirements
- adaptation of release markings
- patch installation
- system software upgrades

Service Flavours: Gateway Security Services comprise of the following flavours:

- **Firewall** covers LAN-WAN or Segmentation gateways; it can include NIPS integration or the establishment of Client to Site or Site to site VPNs

- **Mailguard** covers the secure email exchange between NATO and Mission networks (as part of an Information Exchange Gateway (IEG-C))
- **Guard** covers the secure data exchange between NATO and Mission networks (as part of an Information Exchange Gateway (IEG-C))
- **Data Diode** covers the unidirectional flow of data from a network with a lower security classification to a network with a higher security classification
- **VPN** covers the support of Community of Interest (COI) separation on the NATO Secret network
- **IEG-C** covers additional secure data exchange mechanisms (Web Proxy and RDP Proxy) between NATO and Mission networks, delivered by the NSP008648 project.

Service Available on:

Public Cloud
NATO Unclassified/Restricted
NATO Secret
NATO AOM networks

Service Prerequisites: Gateway Security Services depend on the installation of appropriate network infrastructure.

Standard Service Support Levels:

Service Availability: 24/7

Service Restoration: 2 working days

Maintenance Services: Tuesdays and Thursdays between 19:00 to 21:00 local time. SEC011 might be unavailable at selected sites in order to perform system maintenance and/or upgrades of the underlying operating systems

Support hours: Support hours: Triage and troubleshooting 24/7 via Cyber Security OPCEN (NCN 626 666, see service SEC008). Deep expertise is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time).

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC012 CIS Endpoint Protection Support Service

Service ID: SEC012

Service Name: CIS Endpoint Protection Support Service

Portfolio Group: Security Services

Service Description: Provision of expert guidance for the implementation, configuration and management of NATO Enterprise-wide endpoint security software. This guidance is used to harden NATO CIS against attack and compromise.

The endpoint security guidance consists of the following mandatory/optional controls, as per C3B Technical and Implementation Directive on CIS Security (AC/322-D/0048-REV3):

- Endpoint antimalware
- Host-based Intrusion Prevention (IPS)
- Secure web-browsing
- Desktop Firewall
- Application whitelisting
- Central management control for endpoint management
- Removable media protection
- USB Device Control protection
- Data-in-use Leakage Prevention
- Data-at-rest encryption
- Email antimalware
- Rogue Systems Detection
- Secure media erasure

This service only includes the Agency's centralised resources required for delivery. Local support from collocated staff in support of day-to-day operations is not included and must be funded locally.

Value Proposition: Support to Cyber Security – Prevent. The provision of CIS Protection Support enables coherent implementation of enterprise-wide endpoint security software, aligned to the policies and requirements of NATO that hardens the NATO CIS against compromise and is a proven way forward to increase/maintain security.

Service Features: The use of deep, niche expertise to deliver guidance for the implementation, configuration and management of NATO Enterprise-wide endpoint security software.

It includes:

- Full life cycle management for the respective endpoint security controls, ensuring the Approved Fielded Product List (AFPL) is updated.
- Reviewing and adapting the recommended configuration and guidance for every new minor and major release.
- Monitoring the threat landscape for emerging threats and provide mitigation at endpoint protection level.

- Monitoring the developments in endpoint protection and taking steps towards improving the cyber security controls.
- Reviewing and adapting the guidance for every new minor and major release.
- Providing 3rd-level technical support
- Assisting with vulnerability remediation, as suggested by local CIS Security Officers or revealed from a vulnerability assessment.

Service Flavours: The Service is available as a single flavour.

Service Available on: Network neutral

Service Prerequisites: N/A

Standard Service Support Levels: N/A

Service Cost / Price: The service is unitised based on the number of endpoints (workstations, servers, physical or virtual). For the price details, see the Service Rates document

SEC013 Crypto Compliance Support Service

Service ID: SEC013

Service Name: Crypto Compliance Support Service

Portfolio Group: Security Services

Service Description: Crypto Compliance Support Service provides assessment for Crypto Logistic Support and Maintenance and COMSEC Account management. It does this by providing formal inspections of all organisations storing, operating or maintaining NATO funded cryptographic equipment and NATO COMSEC Accounts in order to ensure compliance with established Directives.

Value Proposition: Cyber Security – Assess. Compliant cryptographic and communication security underpins the cyber security required within NATO and within the Allies. This service provides assurance that cryptographic installations are compliant with appropriate directives procedures and practices of COMSEC account custodianship are compliant with appropriate directives.

Service Features: The Service is comprised of the following elements:

> **Crypto Logistic Support, COMSEC Account and Maintenance Inspections**: Provision of formal inspection of all organisations storing, operating or maintaining NATO funded cryptographic equipment in order to ensure that the procedures and practices of account custodianship, cryptographic logistic support, installation and maintenance is compliant with established Directives.

Service Flavours: The Service is available as a single flavour.

Service Available on:

> NATO Secret
> NATO AOM Networks

Service Prerequisites:

> Appropriate crypto and network access authority.

Standard Service Support Levels: N/A

Support Hours: Triage and troubleshooting 24/7 via Cyber Security OPCEN (NCN 626 6666, see service SEC008). Deep expertise is available during normal business hours (Mon-Thurs 08.30-17.00 Fri 08.30-15.00 Local Time).

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC014 Crypto Management and Logistic Support Service

Service ID: SEC014

Service Name: Crypto Management and Logistic Support Service

Service Type: Customer Facing Service

Portfolio Group: Security Services

Service Description: This service delivers management and logistic support required to securely implement and operate NATOs crypto solutions. This includes the management of the CARDS, EKMS, NEKMS, DKMI and Data at Rest IA Services, the Operational Control of the Crypto Forward Support Points and Cryptographic Keying Material Distribution, expert Device Procurement Support, and crypto integration and validation support.

This service only includes the Agency's centralised resources required for delivery. Local support from collocated staff in support of day-to-day operations is not included and must be funded locally.

Value Proposition: Support to Cyber Security – Prevent. Reliable management of crypto forward support. Delivery of authoritative functional, cryptographic expertise. Enabling of policy compliance and security, and the confidentiality, integrity and availability of data at rest.

Service Features:

CARDS, EKMS, NEKMS and DKMI Services

- Provision of resources to deliver the NATO wide accountability, receipt, transfer, supersession and destruction of cryptographic keying material and equipment.
- Maintenance of the CARDS Servers and authorisation for CARDS access to COMSEC custodians.
- Provision of specialist advice on cryptographic equipment installation, configuration, keying, operation, trouble shooting and related technical or engineering issues.
- Provision of the main point of entry for DACAN Key Management Infrastructure (DKMI) into NATO. Interface for DKMI to NATO EKMS (NEKMS) for NATO wide distribution of crypto electronic keys.

Data at Rest IA Services

- Provision of NATO Offline Crypto Equipment (NOLCE) keying Authority. Distribution and keying of all NATO Offline systems (Eclypt, SIR, Flagstone, etc.).

SECTRA Secure Voice Mobile Key Support

- Key Generation (KGC)
- Crypto Key and SECTRA Device management
- Assist remote sites during the keychange
- Replacement and re-introduction devices into the network
- Manual rekey of existing devices

Crypto Management and Logistic Support

- Cryptographic Device Procurement Support
  - Advice on the design scope and planning for the procurement of NATO-approved cryptographic solutions, and execute the procurement and potentially provide the related services: implementation, training and maintenance.
- Operational Control of the Crypto Forward Support Points.
  - Provides Operational Control and Management of the Crypto Forward Support Points NATO-wide. Provision of timely replacement equipment and testing of faulty equipment prior to evacuation into the maintenance chain.
- Cryptographic Keying Material Distribution
  - The timely distribution of operational keying material and equipment to the end-user.
  - Allocation of keys to service requests (SRTS).
  - Provision of Controlling Authority services for all operational (theatre) and most operational (non-theatre) physical and electronic keying material.
  - Centralised management of distributed Crypto IP equipment providing the encryption of classified data (up to CTS level).

Cryptographic Integration Services

- Installation Site Survey: Provision of Initial Site Surveys in order to deliver specialist implementation and physical security advice prior to installation of cryptographic equipment or implementation of systems with a cryptographic component.
- Cryptographic Equipment Installation: Installation of Cryptographic Devices within Alliance and also individual Nations for end to end encryption ensuring installation and operation complies with current regulations, standards and directives. Installation of all types of cryptographic equipment, to include Voice, IP, Link, Trunk and Wide-Band.
- Production of IP Data Configuration Sheets: Production of user configuration data sheets for IP encrypted links.
- CIS System Management Support: Support to NCI Agency System Managers (and others) in the location, installation and on-site trouble shooting of systems, which include, but are not limited to, NNCCRS, SIGINT COINS, NNPS, NSWAN.

Cryptographic Validation Services

- Installation Inspection: Provision of installation compliance inspections and/or advisory visits on cryptographic installations in order to ensure compliance with current regulations, standards and directives.

Cryptographic Situational Awareness Service – (cost not included in v9.0 Service Rate)

Provision of Enhanced orchestration and maintenance of situational awareness by providing a tool (CSAT) to enable the following operational objectives:

- Provide a clear overview of cryptographic products and mechanisms currently in use.

- Enable the authorized users to perform orchestration of cryptographic activities ensuring management of products /capabilities during their entire life cycle.
- Support the production of operational impact analysis on current / future crypto capabilities as well as the definition of suitable operational mitigation / contingencies,
- Integrate information available in existing Authoritative Data Sources (ADS) to aid in the evaluation of the effectiveness and efficiency of cryptographic products available for NATO usage, as well as of the issues and risks associated with those currently in use.
- Incorporate an inventory of cryptographic products / mechanisms, allow the automatic production of the cryptographic issue mitigation action plan (CIMAP), and include a risk register to provide the commander with the ability to track status and take action as necessary.
- Provide the cryptographic stakeholders with an electronic “one stop shop” for cryptographic information by tracking (or providing links to) the following types of information (both in general for NATO-owned equipment and for national equipment that the nations want to have considered for future NATO use):

    - Inventory of algorithms and their lifetime / expectancy;
    - Approved crypto equipment;
    - Inventory of in-use crypto equipment;
    - Robustness assessment;
    - National notifications of decertification, such as end-of-life; and Issues and risks.

Review of Academy Cryptographic Courses

- Annual review of three cryptographic courses (A0004, A0006, A0067) that are delivered at the NCI Academy to confirm the courses continue to be fit for use and fit for purpose.

Coverage of CyOC Crypto Controlling Authority (CA) Duties

- In the absence of CyOC Crypto SME, NCIA NCSC will take over the following CyOC Crypto Controlling Authority responsibilities:
    - Take action on AIFS/AIMS formal messages addressed to SHAPE CyOC;
    - Authorize decrease/increase of Crypto keymat;
    - Take appropriate actions on COMSEC incidents.

Service Flavours: The Service is available as a single flavour.

Service Available on:

NATO Secret
NATO AOM networks

Service Prerequisites: Appropriate crypto and network access authority. Maintenance, repair of Crypto Equipment. Replacement of faulty crypto equipment on operational circuits. NATO wide Crypto delivery, accounting and key distribution system. The Data at rest IA Service is dependent on available and trained staff to operate, distribute crypto material.

Standard Service Support Levels:

Service Availability: N/A

Service Restoration: 2 working days

Support hours: Triage and troubleshooting 24/7 via Cyber Security OPCEN (NCN 626 6666, see service SEC008). Deep expertise is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time).

Service Cost / Price: The unit of measure for the Service is 1, meaning that the cost/price of the service is calculated on the enterprise total cost basis.

The service description is updated to include Cryptographic Situational Awareness in CCSC v9.0, however cost not included in v9.0 Service Rate. Pending confirmation from requirement owner.

SEC015 Security Certificate Service

Service ID: SEC015

Service Name: Security Certificate Service

Portfolio Group: Security Services

Service Description: Provides Certificate Authority, Revocation and Lifecycle Management of digital certificates/entities, including the appropriate training of registration authority personnel.

This service only includes the Agency's centralised resources required for delivery. Local support from collocated Agency staff in support of day-to-day operations is not included and must be funded locally.

Value Proposition: Support to Cyber Security – Prevent. Secure connection and to authentication through digital certificate creation and management.

Service Features:

Certificate Authority Services for NS / MS, NU / NR and NMS: A service used for the creation and issuance of digital certificates to end-user (both human and non-human). This is service will be provided from a Registration Authority (RA). The RA will be only interface to the NATO PKI system to create and issue digital certificates. The service provided also includes the revocation process. RA's will be installed locally to provide services to the end user both human and non-human. Manpower to operate Registration Authorities situated outside of the NATO Command Structure is not included within this service line. Manpower to operate Registration Authorities for non-eligible entities or exceptional-eligible entities not co-located with a NCS sites shall be provided by those external agencies or multinational entities.

Revocation services to NS / MS, NU / NR and NMS: CRL and OCSP services to NS/MS, NU/NR and NMS is a service used for providing a valid Certificate Revocation List and OCSP responses to end users, both human and non-human. The CRL provides a list of revoked certificates, this list will be checked, every time an end user uses digital certificates to establish a secure connection, or to authenticate to a system the CRL is checked. As soon as a certificate is on the CRL the connection, authentication is denied. OCSP responses provide the validity of a single end entity including the full chain in response to a specific query. The OCSP and CRL services to the aforementioned networks are a vital and critical service.

Lifecycle Management of Digital Certificates / Entities: Lifecycle Management of Digital Certificates / Entities is a service which contains the creation, issuance, management, maintenance, re-issuance, key recovery, revocation and deletion of a bonafide end-user (both human and non-human). The lifecycle management of digital certificates / entities also includes the partial management, maintenance of the meta directory on which the user are created.

Training of Registration Authority Personnel: Training of Registration Authority personnel is a service used for on the job training of Registration Authority Operators

(RA Operators). On the job training takes place after the local site received a RA and the RA is configured and operational.

Service Flavours: The Service is available as a single flavour.

Service Available on:

NATO Unclassified
NATO Restricted
NATO Secret
NATO AOM Network
NMS

Service Prerequisites:

The connectivity to the Certificate authority on the desired network. The system is also dependent on available and trained staff to operate the RA.

Standard Service Support Levels:

Service Availability: N/A

Service Restoration: 2 working days

Support hours: Triage and troubleshooting 24/7 via Cyber Security OPCEN (NCN 626 666, see service SEC008). Deep expertise is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 Local Time).

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC017 Crypto Assessment Support Service

The Service has been consolidated under SEC014 – Crypto Management and Logistic Support Services.

SEC018 Cyber Security Project Management Service

The Service has been consolidated under SEC020 – Cyber Security Management Service.

SEC019 Cyber Operations & Exercises

Service ID: SEC019

Service Name: Cyber Operations & Exercises

Portfolio Group: Security Services

Service Description: This service includes the contribution to the planning, coordination for, and execution of mission-based, cyber technical activities, in support of either a NATO exercise or operation. The service is provided though two distinct service flavours: through the participation of a generalist Cyber Planner (coordinator) in and towards the aforementioned activities contributions by a cyber-subservice specialist SME/capability, principally supporting exercises and DCO activities.

This service only includes the Agency's centralised resources required for delivery. Local support from collocated staff in support of day-to-day operations is not included and must be funded locally.

Value Proposition: Support to Cyber Security - Sustainment. Centralised SME services offer good value by having expert planning and coordination and leveraging the synergies of collocated deep skillsets. These also offer the efficiency of having cyber specialists available and resourced only when the customer requires them to contribute to cyber security sustainment and capability development.

Service Features: Cyber Operations and Exercise Service is comprised of the following elements:

1. **Cyber Security Support to Exercises:** Through a single point of contact coordinate the delivery of Cyber Security protection services and provide exercise development support for exercises identified within the CSLA in addition to the following, cyber-specific exercises:

   Locked Shields
   Cyber Coalition

   Activities may include:

   - Development of realistic and up to date cross-exercise technical storylines that facilitate the simulation of operational consequence management, simulate impact mission assurance and generate operational-level decision-making;
   - Coordinate the alignment of cyber elements between exercises;
   - Coordinate Cyber Security related concept development and experimentation during exercises;
   - Coordinate operational exercise-support services (including NCSC Training Audience);
   - Role simulation and exercise control activities;
   - Coordination of Real life Cyber Security protection services in support of exercises including Gateway Security, Crypto management, Security Certificates, Incident Management and RRT.

The scale of these services provided to an exercise activity is subject to appropriate resourcing to meet the requested support, conducted through an agreed program of work.

2. **Support to Defensive Cyber Operations (DCO):** Comprehensive cyber defence policy has identified Defensive Cyber Operations (DCO) as a joint responsibility of the NATO Office of the CIO (OCIO), CyOC, and NCI Agency. This service flavour provides a counterpart to CyOC and OCIO in order to:

    - Receive, in a general manner, assistance and support in understanding how effective DCOs can be;
    - Receive, in case of a request for DCO, the possible technical options NCIA could leverage with pros and cons and the side impacts;
    - Upon approval of NCIA GM or any other authorized authority, execute and monitor the execution of DCO on NCIA networks;
    - Confirm with CyOC the expected effect is achieved and regular reporting on the effectiveness;
    - Monitor the NCIA-managed network to ensure no unplanned adverse effect are happening;
    - Coordinate termination of the DCO when requested proof reading and drafting of the final report.

Service Flavours: The Service is available as two service flavours: a generalist Cyber Planner as a planning resource and effects coordinator; or as needed, a subservice SME and their more specialized contributions towards an exercise or operation.

Available on: Network neutral

Service Prerequisites:

None

Standard Service Support Levels:

Service Availability: Not applicable.

Service Restoration: Not applicable.

Service Cost/Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC020 Cyber Security Management Service

Service ID: SEC020

Service Name: Cyber Security Operations Management Service

Service Type: Supporting Service

Portfolio Group: Security Services

Service Description: Cyber Security Operations Management Service underpin and enable the delivery of the other NATO Cyber Security Centre (NCSC) Services.

Value proposition: Cyber Security Operations Management Service facilitate the effective, efficient and resilient delivery of all other NCSC services. The service provides the essential capabilities that underline the provision of NCSC's portfolio of Cyber Security Services, in particular the people, resource, materiel and management essential to their operational delivery.

Service Features:

Acquisition Support: Acquisition support activities to procure the necessary external CIS required for the delivery of NCSC's cyber security services in compliance to NATO Financial Regulations for transparency and competitiveness. This may include the procurement of annual hardware support and software licenses, professional support services, outsourced support contracts, and consumables and sundry items.

Business Management Support: Planning and execution of NCSC business, financial, resource, logistics, training coordination, operational deployment planning, travel, and personnel related activities. Review, creation, maintenance, distribution, and advising on NCSC business, financial, resource and personnel planning project plans and documents. Coordination of NCSC logistic requirements, development and management of the NCSC budget, leading the submission of Medium-Term Financial Plan (MTFP) bids and management of all procurement requirements. Includes NCSC level travel coordination and liaison.

Service Delivery Management Support: Acting as a source of expertise and single point of entry for NCSC Service Level Management activities, including: service catalogue and Service Level Agreement (SLA) reviews, formation of metrics and KPIs, monthly and quarterly reporting, contingency planning, change management, and configuration management. Liaison with internal and external customers to ensure mutual agreement on the evolution of NCSC's services.

Project Management Support: Management of projects according to PRINCE2 methodology. This service includes the definition of acquisition requirements and contracting strategy, followed by a competitive outsourcing to industry from the 30 NATO nations. It includes as well partnering with industry to ensure that the latest, state-of-the-art technology is implemented in a coherent and cost-effective way.

Architecture Support: Architecture expertise to ensure the evolution of NCSC services are coherent with the overarching direction of NATO's technical CIS architecture.

Assessment of customer requests and solution approach to recommend the set of NCSC services necessary to be compliant to NATO security directives.

Internal IKM and Administrative Support: Cyber Security Information Knowledge Management: Management of the content of all the data-centric CIS Security systems, ensuring the coherence and the accuracy of all the data stores used by CIS Security Capabilities. Day-to-day administrative support to ensure smooth operation within the NATO Cyber Security Centre.

Service Request: Inherent to delivery of other NCSC Cyber Security Services.

Service Flavours: Service is available as a single flavour.

Available on: Network neutral

Service Prerequisites: None

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC021 DCIS – Signal Support Group (SSG) Service

The Service has been consolidated under the INF035 DCIS – Deployable Nodes Service.

SEC022 Application Layer Firewall for Sensors and Flight Plans (ALF-SFP) Security Service

Service ID: SEC022

Service Name: Application Layer Firewall for Sensors and Flight Plans (ALF-SFP) Security Service

Portfolio Group: Security Service

Service Description: The Application Layer Firewall for Sensors and Flight Plans(ALF-SFP) is an AirC2 specific service and secures the interconnection of Sensor and Flight Plan data sources provided at lower level of classification with Air Command and Control Systems (AirC2 systems). The ALF-SFP has been initially developed to satisfy requirements to secure the Air Command and Control System (ACCS) system boundary for sensor and flight plan data exchange but can be utilized for any other Command and Control System used in the Air Domain. In principle, the Service is leveraging a secured Trusted Computing Base providing hardening as well as Application Layer Firewall functions for a variety of similar security appliances. The ALF-SFP service is relying on a secured operating platform, data syntax validation and a hardened Application Layer Firewall. The Service provides unidirectional data flow from lower to higher level of classification as required to operate ACCS.

The ALF-SFP falls under the AirC2 governance for programmatic and configuration control aspects. In regard to cyber security evaluation and approval to operate, the ALF-SFP Security Service is under oversight of the ACCS Security Accreditation Board which might call for SECAN evaluation when deemed necessary.

Value proposition: Cyber security support to ensure integrity of sensor and flight plan data exchanged with the Air C2 System as well protecting the security boundary of the Air C2 system in regard to the interfaces supported.

Service Features:

The ALF-SFP is built on a secured Solaris platform utilizing the NISP Service (PLT013) and comprises a message syntax validation through proxies and an Application Layer Firewall as an evaluated security enforcing capability including required secured access to manage required components and interfaces.

The ALF-SFP service can be deployed and used in two scenarios:

- Stand-Alone ALF-SFP: The ALF-SFP supports handling and forwarding Eurocontrol ASTERIX and NATO STANAG 5535/ ADatP-35 compliant messages, as supported by ASIM (INF028), and it supports ICAO compliant Flight Plan Messages, as required for ACCS (APP050).
- ALF-SFP Service combined with ASIM (INF028) to ensure integrity of sensor data and to protect system boundaries against cyber threats.

Service Flavours:

- ***NCS wide ALF-SFP*** single SW baseline maintenance and In-Service-Support (ISS). The NATO ALF-SFP baseline maintained with this service flavour is a prerequisite for all other service flavours.
- ***Site specific ALF-SFP*** integration customised to local site specific requirements outside the NCS.

The ALF-SFP Service can be combined with ASIM (INF028) for sensor integration as required for the connected AirC2 system consuming sensor and flight plan data.

Available on:

NATO Secret to operate security protection functions and to connect to the AirC2 system and

NATO Confidential for Military sensor data sources and

NATO Unclassified for civilian Sensor and flight plan data sources.

Service Prerequisites:

PLT013 - NISP Service providing the standardized secured operating system
INF028 - ASIM Service either at the high or low side when combined with this security service

Hardware, software and connection requirements:

- Sensor data available at IP network level
- IP interface as part of the ACCS or Air C2 system
- Server hardware compatible to run NISP and authorized to host the ALF-SFP
- Network infrastructure

Standard Service Support Levels:

Support Hours:

Centralised Service Desk specialist agents are available during:

- Monday to Thursday: 0600 to 2200 (CET)
- Friday: 0600 to 2000 (CET)

Outside of these hours, calls to the CSD will be answered by 24/7 duty Enterprise Services Operations Centre (ESOC) personnel who will record the Incident/Service Request and take escalation action if necessary.

Standard 2nd and 3rd level support is available during normal business hours (Mon-Thurs 08.30-17.30 Fri 08.30-15.30 CET).

Incident/problem reporting:

Please contact the Centralized service desk: 626 3177 (NCN) or the commercial number

- Belgium +32 65 44 3177
- Netherlands +31 70 374 3177
- Italy +39 081 721 3177

- Germany +49 282 4978 3177
- USA +1 757 747 3177
- For NATO HQ +32 02 707 5858

Service Requests:

To request the SEC022 service, please complete the Customer Request Form and contact NCI Agency through the submit function included in the form following the link below.
https://www.ncia.nato.int/Documents/Customer_Request_Form.pdf

KPIs:

Functional unit	Service Level Target (availability)	Performance Thresholds
ALF-SFP single instance	99.5%	30 ms delay for passing data between ACCS and external systems

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical or high incident (i.e. P1/P2) is 1 day. For medium incidents (P3) it is 3 days.

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. Service levels will be defined per customer according to the customer requirements and the corresponding POW or SLA applicable in each case.

Service Cost / Price: The unit of measure for the Service is 1. Service Initiation and In-Service-Support will be provided and charged in accordance with the scope and financial estimates developed and agreed through site specific Technical Agreements.

Service ID	Service Name	Service Flavour/Option	Service Unit of Measure
SEC022	Application Layer Firewall for Sensors and Flight Plans (ALF-SFP) Security Service	NCS wide ALF-SFP software baseline maintenance and In Service Support (ISS)	1
SEC022	Application Layer Firewall for Sensors and Flight Plans (ALF-SFP) Security Service	***Site specific ALF-SFP*** installation	1

SEC023 Penetration Testing Service

Service ID: SEC023

Service Name: Penetration Testing Service

Portfolio Group: Security Services

Service Description: The Penetration Testing service seeks to test and improve resilience, assess compliance to security standards and identify vulnerabilities of NATO Communication Systems and Networks, through tailored security evaluation of CIS, websites, customer sites and communication equipment, in order to inform customers of existing vulnerabilities, allow remediation to occur and improve their security posture.

Value Proposition: Support to Cyber Security - Assessment. Principally, this service enables the customer to have a better understanding of their vulnerabilities and be able to remediate them before they can be exploited. Understanding vulnerabilities and resilience provides the necessary information to build an accurate picture of the security posture, and creates a baseline to measure progress of security improvements.

Service Features:

Penetration Testing (NATO Type 4 Security Audit): Tailored security tests against NATO networks and systems, with the objective to assess the impact of current cyber threats and techniques, as well as, their likelihood and difficulty of exploitation, on NATO CIS, a NATO Mission or NATO's cyber defences by emulating an intermediate or advanced cyber adversary. These unique activities are performed in support of accreditation, IT change management and software development assurance throughout the lifecycle of NATO CIS. A findings report is generated and provided to the customer at the conclusion of the test.

Service Flavours:

Penetration Testing could be tailored to different systems and production and pre-production environments, depending on customer's needs.

- **Web Application Penetration Test –** This test focuses on evaluating the security of a web application by simulating an attack from an unauthorized user or hacker. The aim of this test is to identify vulnerabilities, misconfigurations, and weaknesses in the web application, and to provide recommendations to improve its security posture. The engagement can vary in scoping/size, as outlined below:
  - **Small**: web application - simple/basic functionality - minimal number of users - simple architecture
  - **Medium**: one or several web application with common features, login/user permissions/file upload/ and medium number of users - n-tier architecture
  - **Large**: Several number of complex web applications - with n-tier architecture, including middle ware and back-end application - rich featured - large user base
  - **Regression test**: re-test focused on the previously identified issues

- **OWASP ASVS Compliancy**: Compliancy check of the web application with the latest OWASP ASVS standard.

- **Network/Infrastructure Penetration Test –** This test focuses on evaluating the security of a network/infrastructure by simulating an attack from an unauthorized user or hacker. The aim of this test is to identify vulnerabilities, misconfigurations, and weaknesses in the network and infrastructure, and to provide recommendations to improve its security posture. The engagement can vary in scoping/size, as outlined below:
  - **Small**: typically one target (web application/application/server)
  - **Medium**: n-tier architecture, with several servers (presence of middle-ware components and back-end)
  - **Large**: complex network environments/AD/large number of users/applications/protocols/ and cross domain architecture
  - **Regression test**: re-test focused on the previously identified issues

- **Application Penetration Test –** This test focuses on evaluating the security of an application/software by simulating an attack from an unauthorized user or hacker. The aim of this test is to identify vulnerabilities, misconfigurations, and weaknesses in the application, and to provide recommendations to improve its security posture. The engagement can vary in scoping/size, as outlined below:
  - **Small**: single target / simple/basic functionality – minimal number of users – simple architecture
  - **Medium**: one or several applications – medium-size user base
  - **Large**: several number of complex applications, protocols and/or daemons – large-size user base
  - **Regression test**: re-test focused on the previously identified issues
  - **Light**: Quick check aimed to verify presence of backdoor, spyware, outdated software only.

Service Available On:

NATO Unclassified
NATO Restricted
NATO Secret
NATO AOM networks

Service Prerequisites:

None

Standard Service Support Levels: N/A

Service Cost / Price: The service is unitised based on the service flavour, with the unit of measure is per testing based on the complexity of the scope to be assessed or the type of test to be performed. For the price details, see the Service Rates document.

SEC024 Vulnerability Assessment Service

Service ID: SEC024

Service Name: Vulnerability Assessment

Portfolio Group: Security Services

Service Description: The Vulnerability Assessment Service seeks to test and improve resilience, assess compliance to NATO and industry security standards and identify vulnerabilities of NATO Communication Systems and Networks. It accomplishes this by the provision of resources to deliver on premise, holistic technical vulnerability assessments to support the identification, quantification and prioritization of Cyber security risks and vulnerabilities in computer networks, systems (including Industrial Control Systems), hardware and applications. Then, informs the customer of existing vulnerabilities allowing remediation to occur to improve their security posture.

Value Proposition: Support to Cyber Security Assessment. Vulnerability Assessments comply with NATO Security Policy and Directive that requires periodic Cyber Security Audits and supports Security Accreditation Authorities make risk informed decision during the accreditation process. It helps the customer implement gradual risk reduction measures through identifying risks and recommends the strategical remediation of vulnerabilities by the combination of threat-based and risk-based approaches. The assessment prioritizes vulnerabilities in their context of exposures, using critical, attack-centric risk context such as the applicability of each vulnerability to threats, their potential impact on the organization and its mission, asset criticality and accessibility.

Service Features:

Onsite Vulnerability Assessment (NATO Type 3 Security Audit):

Execution of in-depth technical vulnerability assessments for NATO CIS networks against current threat landscape, NATO Policies & Directives, with root cause analysis, reporting and recommendations for remediation and mitigation.

Includes the execution of the following checks:

- Inventory and security control of enterprise assets
- Inventory and security control of software assets
- Assessment of data protection security
- Assessment of secure configuration of enterprise assets and software
- Assessment of authentication, authorisation and account security management
- Assessment of access control management
- Assessment of vulnerability (management) status
- Assessment of audit log management
- Assessment of email and web browser protections
- Assessment of malware and endpoint security defences
- Assessment of data recovery
- Assessment of network infrastructure security management
- Assessment of network monitoring and defence

Service Flavours: The service is unitised based on five variations (XS, S, M, L, XL), with the determination of the variation based on the complexity of the scope to be assessed. The Service Delivery Manager reserves the right for final determination.

1. **SEC024-1:** Small (XS) | one network, <35 IP assets
2. **SEC024-2**: Small (S) | two networks, <100 IP assets per network
3. **SEC024-3:** Medium (M) | two or three networks, <200 IP assets per network
4. **SEC024-4:** Large (L) | three networks, <500 IP assets per network
5. **SEC024-5:** Extra-Large (XL) | three networks, <850 IP assets per network

Service Available On:

NATO Unclassified
NATO Restricted
NATO Confidential
NATO Secret
Cosmic Top Secret
NATO AOM networks

Prerequisite Services:

None.

Standard Service Support Levels: N/A

Service Cost / Price: The service is unitised based on five variations (XS, S, M, L, XL), with the determination of the variation based on the complexity of the scope to be assessed. For the price details, see the Service Rates document.

SEC025 Emission Security Service

Service ID: SEC025

Service Name: Emission Security Service

Portfolio Group: Security Services

Service Description: The Emission Security Service seeks to assess compliance to standards and identify vulnerabilities, through the electronic evaluation of facilities processing classified information to establish their Facility Zone rating and subsequent vulnerability assessment of compromising emanations, in order to allow remediation to occur.

This service only includes the Agency's centralised resources required for delivery. Local support from collocated Agency staff in support of day-to-day operations is not included and must be funded locally. The Agency is working towards consolidation of these local support costs into this service for the future years.

Value Proposition: Support to Cyber Security - Assessment. Principally this service enables the customer to have a better understanding of their vulnerabilities and so be able to remediate them before being exploited. Being able to understand any vulnerabilities and strengths also supports being able to build a picture of overall security, creating a baseline for measure progress to security improvements.

Service Features:

> **TEMPEST Facility Zoning:** Provision of electronic evaluation of Facilities and Buildings where Classified information is processed in order to determine their Facility Zone Rating. Including advice to local IA staff on TEMPEST issues. The zone rating is provided with a technical report.
>
> **EMSEC Vulnerability Assessment:** Provision of EMSEC vulnerability assessment within a Zoned Facility. The service includes advice to local IA staff on TEMPEST issues. The findings of the assessment is provided as a report.

Service Flavours: The Service is available as a single flavour.

Service Available On:

NATO Unclassified
NATO Restricted
NATO Secret
NATO AOM networks

Service Prerequisites:

None

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC026 Attack Surface Reduction Service

Service ID: SEC026

Service Name: Attack Surface Reduction Service

Service Type: Customer Facing Service

Portfolio Group: Security Services

Service Description: The Attack Surface Reduction Service provides Security Baselines, Vulnerability Monitoring and awareness, and Supply Chain Cyber Security. It delivers up-to-date Security Hardening Guides and support regarding their application to NATO CIS, analysis and evaluation of the recently discovered vulnerabilities affecting software and non-software CIS elements, and provides ad-hoc expertise related to CIS Component trustworthiness to system owners for their NATO CIS.

This service only includes the Agency's centralised resources required for delivery. Local support from collocated staff in support of day-to-day operations is not included and must be funded locally.

Value Proposition: Support to Cyber Security – Prevent. Security Hardening guides provides the NATO security baseline and minimal security posture required for a secure CIS, as per NATO directives and security best practices. Vulnerability management enables appropriate awareness of the CIS community related to the risk exposure NATO CIS is facing on a daily basis. Supply Chain Cyber Security constitutes an ad-hoc expertise capability, evaluating the level of trust that can be placed on a CIS component, based on the underlying deployed security measures in support of its development and maintenance.

Service Features:

Security Hardening Support: This service feature produces, delivers and maintains Security Guides for Software and Non-software products (Operating Systems, appliances) as part of the NCIA Change Management process. As such, Security Hardening guides constitute the minimal security baselines a CIS shall comply with. It also provides support to stakeholders on implementing the Security Guide on NATO CIS

Vulnerability Monitoring and Awareness: This service feature is composed of Monitoring of Vulnerability and Patch notification feeds and information channels; it assess relevance of known vulnerabilities to NATO CIS and to which extent they represent a risk for the organisation. The service includes publication of Weekly Security Bulletins which are relevant for NATO CIS, and Ad-hoc Security Bulletins which are relevant for NATO CIS (assessment of relevance to NATO, risk level exposure, identification of existing exploits, possible mitigations and remediation actions, recommendations regarding actions to be taken, identification of possible side effects and additional risks). The service also participates in NCIA patch management processes, including the "battleshort" procedure.

Supply Chain Cyber Security: Plan for, collect information about, assess, and handle the level of trust that can be placed in the components of a CIS based on the supply of sub-components, manufacturing, and logistics.

Service Flavours: The Service is available as a single flavour.

Service Available on:

NATO Unclassified
NATO Restricted
NATO Secret
NATO AOM networks

Service Prerequisites: N/A

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC027 Continuous Security Posture Assessment Service

Service ID: SEC027

Service Name: Continuous Security Posture Assessment Service

Service Type: Customer Facing Service

Portfolio Group: Security Services

Service Description: The Continuous Security Posture Assessment Service delivers the External Attack Surface Monitoring and Online Vulnerability Assessment services. It seeks to assess compliance to standards and identify vulnerabilities on CIS components, communicate the results to the service owners, provides advice and expertise on the appropriate resolution paths, and engage the remediation process.

This service only includes the Agency's centralised resources required for delivery. Local support from collocated staff in support of day-to-day operations is not included and must be funded locally.

Value Proposition: Support to Cyber Security - Assessment. This service contributes to the good standing of Cyber Security Hygiene Indicators, by measuring the level of exposure to vulnerabilities of networked CIS components. It enables the remediation processes by identifying security shortfalls and delivering a mostly automated vulnerability picture from various potential points of attacks, together with a level of expertise regarding applicable protection measures to support reducing the potential attack surface.

Service Features:

External Attack Surface Monitoring: Provision of resources to continually assess the exposure of NATO CIS to the Internet. The findings and remediation recommendations are provided with the assessment report.

Online Vulnerability Assessment and Remediation Support: Provision of Online Vulnerability Assessment resources to carry out continuous and dynamic evaluations / audits of CIS infrastructures / systems to identify any vulnerabilities in software or configurations and to provide detailed reports. Includes the execution of the following checks:

- Inventory of all connected devices
- Inventory of authorized and unauthorized software
- Inventory of patch and update status of all installed software and operating systems
- Data Loss Prevention solution (DLP)
- Secure configurations for hardware and software on workstations and servers
- Malware defences and endpoint security mechanisms status
- Secure configurations for locally managed network devices (limited functionality)
- End of life Operating Systems and Applications
- **Remediation Support:** OVA reports containing cyber security hygiene indicators status, findings and prioritized remediation measures. Advising on mitigation techniques, escalating issues, with the objective of closing vulnerabilities at sites.

Service Flavours: The service is unitised based on four variations (S, M, L, XL), with the determination of the variation based on the complexity of the scope to be assessed. The Service Delivery Manager reserves the right for final determination.

1. **SEC027-1:** Small (S) | one networks, <100 IP assets per network
2. **SEC027-2**: Medium (M) | one network, <500 IP assets per network
3. **SEC027-3:** Large (L) | one network, <1000 IP assets per network
4. **SEC027-4:** Extra-Large (XL) | one network, >1000 IP assets per network
5. **SEC027-5:** External Attack Surface Monitoring

Service Available on:

NATO Unclassified
NATO Restricted
NATO Secret
NATO AOM networks

Service Prerequisites: SEC029 delivers the PaaS to host SEC027.

Standard Service Support Levels: N/A

Service Cost / Price: The service is unitised based on four variations (S, M, L, XL), with the determination of the variation based on the complexity of the scope to be assessed. For the price details, see the Service Rates document.

SEC028 Vulnerability Management Service

Service ID: SEC028

Service Name: Vulnerability Management Service

Service Type: Customer Facing Service

Portfolio Group: Security Services

Service Description: The Vulnerability Management Service provides the coordination of Remediation and Mitigations actions for CIS system owners, following Security Incident, Vulnerability Assessment or Pentesting activities carried out on the targeted systems.

This service only includes the Agency's centralised resources required for delivery. Local support from collocated staff in support of day-to-day operations is not included and must be funded locally.

Value Proposition: Support to Cyber Security – Assess. Vulnerability Management improves the efficiency of the Cyber Security Hygiene Indicators (CSHI) the NCI Agency is maintaining, by facilitating, advising, prioritizing and coordinating with the Security Stakeholders (SAA, CISO, etc.) and systems administrators; providing basic tracking of unresolved priority vulnerabilities.

It constitutes the coordination and vulnerability information aggregation point that enables resolution of identified security shortfalls.

Service Features:

Vulnerability Management: Vulnerability Management Service orchestrates and reports on the vulnerability lifecycle. It:

- Aggregates the NCSC vulnerability sources,
- Identifies possible remediation and mitigation of identified security shortfalls,
- Recommends priorities,
- Initiates the resolution process,
- Tracks and traces the resolution activities
- Closes the loop by verifying the effectiveness of these activities.

Vulnerability Management delivers regular reports, access to dashboards and provide ad-hoc expertise on this particular topic.

Service Flavours: The Service is available as a single flavour.

Service Available on:

NATO Unclassified
NATO Restricted
NATO Secret
NATO AOM networks

Service Prerequisites: N/A

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC029 Cyber Security Platform and Infrastructure Service

Service ID: SEC029

Service Name: Cyber Security Platform and Infrastructure Service

Service Type: Supporting Service

Portfolio Group: Security Services

Service Description: The Cyber Security Platform and Infrastructure Service provides the NCSC Core physical and virtualised CIS infrastructure - covering both Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). These services provide the underpinning building block layer for other NCSC dependent services (Cyber Security Monitoring & Incident Management / Online Vulnerability Assessment / NIPS & FPC / Online & Offline Computer Forensics / E-mail Filtering / Endpoint and E-mail Security). The infrastructure associated with the service is layered in 3 tiers: T1 in NNHQ Brussels / T2 in SHAPE MONS (NCSC core networks and appliances) and T3 (Remote NATO Sites) via dedicated NCSC enclaves.

This service only includes the Agency's centralised resources required for delivery. Local support (Level 1) from remote staff in support of day-to-day operations is enabled under appropriate Operating Level Agreement with the respective NCIA Business Areas.

Value Proposition: Support to Cyber Security – Sustainment. This service is a key enabler that enables NCSC to operate and provide its customer facing services.

Service Features: This service is comprised of the following elements:

- **Cyber Infrastructure-as-a-Service (IaaS):** NCSC's IaaS provides the physical and virtual infrastructure for hosting the set of tools required to deliver NCSC's portfolio of cyber security services.
- **Cyber Platform-as-a-Service (PaaS):** NCSC's PaaS provides the Operating System level hosting for the upper level applications and toolsets required to deliver NCSC's portfolio of cyber security services. This includes back-office functionality - i.e MS Office, E-mail and Business Continuity functions.

Service Flavours: The Service is available in two flavours:

1. **Central Services** – located in Mons, Belgium and constitutes the main Cyber Security Centre Operating capability.
2. **Tier 3 Enclaves** – located at remote Tier 3 sites to enable the effective monitoring, logging, scanning of remote networks.

Service Available on:

- NCSC Core Unclassified
- NCSC Core Restricted
- NCSC Core Secret
- NRoI Restricted

Service Prerequisites:

Provision of HVAC and Accommodation for NCSC central and deployed capabilities.

Standard Service Support Levels:

Service Availability Target: 99.5%

Service Restoration: Where the service is deemed unavailable, the service restoration period for a critical incident (i.e. P0/P1) is shown in the Service Restoration Period table below.[1]

	Availability Target	Service Restoration Period
During Support Hours	99.5%	4 hours
Outside Support Hours	99.5% (critical services)	4 hours

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

[1] Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA. While this provides a standard availability target for the service, regional support arrangements and therefore the availability targets may vary and should be agreed during the SLA discussions.

SEC030 Cyber Threat Hunting Service

Service ID: SEC030

Service Name: Cyber Threat Hunting Service

Service Type: Customer Facing Service

Portfolio Group: Security Services

Service Description: The Cyber-Threat Hunting service provides a threat-based detection and hunting capability through directed analysis of NATO CIS against a selected set of intelligence artefacts, Indicators of Compromise, predicted tactics, techniques and practices of Cyber Threat Actors (CTA), cyber criminals and insider threats. This set of actionable information is provided in a joint effort by SHAPE CyOC, JISD, OCIO and other relevant stakeholders according to the agreed NCSC-developed process. This allows identification of advanced attempts to compromise NATO CIS from threat actors knowledgeable enough to avoid automated detection techniques and provides a technical assessment that will inform the operational assessment and follow-on defensive activities. This service can be provided inside and outside the scope of Defensive Cyber Operations (DCO).

This service only includes the Agency's centralised resources required for delivery. Local support from collocated staff in support of day-to-day operations is not included and must be funded locally. If reinforcement by industry partners is required, the supplemental cost will also be charged separately.

Value Proposition: Support to Cyber Security - Defence. The direct benefit of Threat Hunting is a reduction in average detection time through the proactive discovery of security incidents and/or adverse activity that evade usual detection methods, allowing early and coordinated response.

Service Features:

- **Asset Monitoring:** Configuration, collection and evaluation.
- **Technical Analysis:** Targeted Network Collection, Monitoring and Detection.
- **Correlation:** Tailored evaluation within a dedicated repository, search and analysis of malicious patterns and behaviours.

Service Flavours: The Service is available as a single flavour.

Service Available on:

NATO Unclassified
NATO Restricted
NATO Secret
NATO AOM networks

Service Prerequisites: The execution of the service have technical prerequisites. Depending on the scope of the threat hunting, the necessary tools will need to be installed on the target network(s) and confirmed working before the Threat Hunting can occur.

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC032 Adversary Emulation Service

Service ID: SEC032

Service Name: Adversary Emulation Service

Portfolio Group: Security Services

Service Description: The Adversary Emulation Service seeks to assess and improve the resilience of NATO Communication Systems and Networks, through tailored security evaluation of people, process and technology, in order to allow remediation to occur and improve their security posture.

Value Proposition: Support to Cyber Security - Assessment. Principally, this service enables the customer to assess and improve its resilience against an advanced attacker. Understanding vulnerabilities and resilience provides the necessary information to build an accurate picture of the security posture, and creates a baseline to measure progress of security improvements.

Service Features:

Adversary Emulation (NATO Type 5 Security Audit): Tailored red and purple teaming activities against NATO networks and systems, with the objective to evaluate and improve the resilience of NATO CIS, NATO Mission or NATO's cyber defences by emulating an intermediate or advanced cyber adversary. Adversary emulation mimics specific techniques, tactics and procedures (TTPs) used by known threat actors. Adversary emulators construct scenarios to test different aspects of an adversary's TTPs against a given target. These unique activities are performed in support of NATO missions and exercises. A security report is generated and provided to the customer at the conclusion of the test.

Service Flavours:

- **Red Teaming –** Objective based assessment to test the resilience of a target network, mimicking a malicious actor to assess the people, process and technology in terms of prevention, detection and response to a cyber-threat. In this flavour, the Red team tries to stay as stealthy as possible to assess the prevention, detection and response capabilities of a given target following the "train as we fight" approach.
  - **Small**: Small-scale red team engagement involves a small group of security professionals. The team uses a targeted approach to reach their defined objectives. This type of engagement is usually conducted in one phase of testing over a short period.
  - **Large**: Large-scale red team engagement involves a larger team of security professionals. This type of engagement is usually more comprehensive and can last for several months, during which the team conducts various tests and simulations to reach their objectives. A large red team engagement typically requires more resources, including personnel, time, and

specialized tools and technologies, and may involve multiple phases or stages of testing.

- **Purple Teaming –** Scenario based assessment to test the resilience of a target network, mimicking a malicious actor to assess the prevention and detection to a cyber-threat. In this flavour, the Red team works with the Blue team to assess the prevention and detection of each scenario.
  - **Security controls validation**: determines how effective deployed security technologies are, as an overall system of security systems. The main goal of security control validations is to assess and improve the detection and prevention mechanisms of a given system against TTPs used by threat actors targeting NATO.
  - **Baseline assessment**: benchmarks the detection and prevention mechanisms of a given baseline. The goal of a baseline assessment is to measure the effectiveness of new security technologies implemented on a defined baseline.
- **Phishing Simulation Campaigns –** Provision of resources to configure and execute phishing simulation campaigns directed at all levels of NATO staff. Phishing Simulation Campaigns aim at exposing staffs of all levels to the dangers encountered with modern communications methods and systems, by using the same targeting methods adversaries use with the intention of gathering information of specific target. The findings and remediation recommendations are provided with the campaign reports.

Service Available On:

NATO Unclassified
NATO Restricted
NATO Secret
NATO AOM networks

Service Prerequisites:

None

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

SEC033 Cyber Security Architectural Coherency and Roadmaps

Service ID: SEC033

Service Name: Cyber Security Architectural Coherency and Roadmaps Service

Portfolio Group: Security Services

Service Description: The NATO Cyber Security Centre (NCSC) is responsible for the enhancements and bolstering of NATO capabilities, linked to key NCSC provided services, across a variety of programming vehicles ranging from NATO Security Investment Program (NSIP) activities, minor works activities and URs/CURs. Given these vehicles emerge from various sources, there is a strong need to ensure coherency across various projects and alignment to either new or existing services. Further, any changes (enhancements), applied to services must be done so in a holistic fashion and integrated in a coordinated way with service providers and consumers (NCSC's customer base). Service evolutions must be planned in a similar fashion and maintaining a strategic direction for all of NCSC's services requires regular coordination with key stakeholders within ACT, ACO and the OCIO. By ensuring a strong foundation regarding the anticipated, planned, under way and desired requirements for NCSC services, customer requirements are aligned for future operational requirements and ensure target environments are known for implementation activities. This results in significant efficiency with respect to solutions and their implementations, which allows NCSC to develop coherent, world class solutions that are reflected in continuously updated and accurate service roadmaps to define evolution in accordance with external NATO ambitions such as Digital Transformation, Multi Domain Operations, etc.

Value Proposition: Enabling NCSC Staff to coherently review and consolidate customer requirements against the needs of NATO and develop service roadmaps in order to improve service delivery will result in improved quality, sophisticated solutions and cost efficiencies.

Service Features: Regular review, update, enhancements and documented evolutions of service roadmaps which are aligned with NATO ambitions and customer expectations regarding NATO Digital Transformation, Multi Domain Operations, etc.

Service Flavours: This Service is available as a single flavour.

Service Available on: N/A

Service Prerequisites: None.

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

Training Services

This page is left blank intentionally

TRA002 Education and Individual Training Delivery (EIT Delivery)

Service ID: TRA002

Service Name: Education and Individual Training Delivery

Service Type: Customer facing

Portfolio Group: Training services

Service Status: Available

Service Description: This service manages, coordinates and delivers cyberspace education and training services (EIT) to NATO, the Nations and internal NCI Agency staff. The service delivers training courses and other Education and Individual Training (EIT) opportunities by the NCI Academy, an integral element of the NCI Agency. The full list of services, including a description and features, is available in the NCI Academy Cyberspace Learning Catalogue.

The service includes the provision of a comprehensive Catalogue of Cyber Learning and Curriculum along with the planning, scheduling, quality management and continuous improvement for the delivery and management of the training services listed in the catalogue and support to the students attending them.

This service includes the specialist IT, tools and infrastructure required to manage the service and to deliver on-site, live on-line, self-paced and blended learning.

This service does not include the NATO systems (hardware, software and applications) that are the subject of the respective courses.

This service does not include the training environment for services delivered at the customers' sites or local support from collocated Agency staff for ad-hoc, on-site training events, such as preparation of training facilities, IT training environment etc; such support must be funded separately.

Value Proposition: The training services enable the customer to use, administer and maintain other services and systems provided by the NCI Agency. This service also provides professional development training.

Service Features: The features of this service are available in the NCI Academy Cyberspace Learning Catalogue.

Service Flavours: Training opportunities are available as pre-defined in-house courses at Agency sites, through Mobile Training Teams delivered on-site at customer locations, hybrid learning, live on-line, self-paced on-line or through blended learning Tailored training will also be considered upon request.

Available on: N/A

Service Prerequisites: TRA003: Education and Individual Training Availability and Maintenance. Business prerequisites and prerequisites for individual courses as detailed in the NCI Academy Cyberspace Learning Catalogue.

Standard Service Support Levels*:* N/A

Service Availability[1] Target: N/A

Service Restoration: N/A

Service Cost / Price: Service prices (course prices) are provided as an annex to the NCI Academy Cyberspace Learning Catalogue. Prices for tailored NCI Academy training will be calculated upon request.

[1] The minimum "Monthly Uptime Percentage" for a Service is calculated by the following formula: (Available Minutes* - Downtime) / Available Minutes x 100
**Minutes available during agreed reporting period excluding planned maintenance minutes*

TRA003 Education and Individual Training Availability and Maintenance (EIT A&M)

Service ID: TRA003

Service Name: Education and Individual Training Availability and Maintenance

Portfolio Group: Training services

Service Description: This service maintains the NATO-Required training curriculum delivered through service TRA002: Education and Individual Training Delivery and ensures the availability of professional, certified instructional capacity and the high quality training capability to plan, coordinate and deliver these courses.

Value Proposition: This service mitigates the operational risk to customers that NATO-Required courses are discontinued by the NCI Agency as a result of not breaking even on course prices and ensures that NCS elements have seat allocation priority on those courses. The service reduces the volatility of the course prices and increases the predictability of the annual customer budgets required for Education and Individual Training.

Service Features: N/A

Service Flavours: N/A

Available on: N/A

Service Prerequisites: Maintenance of training systems, including underlying hardware, software and applications, SME or Security Services, on which the Education and Individual Training courses are provided. The operation and maintenance of specialist IT, training management systems, and Learning Management System (JADL) used for on-site, live on-line, self-paced, and blended learning delivery by TRA002.

Standard Service Support Levels*:*

- **Service Availability[1] Target:** N/A
- **Service Restoration:** N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

Logistics Support Services

This page is left blank intentionally

LOG001 CIS Asset & Materiel Management Service

Service ID: LOG001

Service Name: CIS Asset & Materiel Management

Service Type: Customer Facing/Support

Portfolio Group: Logistic Services

Service Description: The CIS Asset & Materiel Management Service embraces all of the CIS Asset and Materiel Management activities that the CIS Sustainment Support Centre (CSSC) provides both directly to the Customer and internally as a support function to the Service Lines. CIS Asset and Materiel Management includes CIS equipment codification, database management, inventory management, receipt, dispatch, storage, stock management, warehousing, internal controls, handover takeover, equipment write-on/write-off, support to operations and disposal coordination. The CSSC performs as the single point of entry for the majority of new CIS equipment procured through common funding of NATO. In addition, CSSC provides Asset Management Subject Matter Expert Services directly to the Customer or internally to the NCI Agency Service Lines.

This service only includes the Agency's centralised resources required to deliver the service. Local support from collocated Agency staff in support of day-to-day operations is not included and must be funded locally.

Value Proposition: The Service provides multiple values:

- Provision of a central hub for most of CIS Asset and Materiel Management activities;
- NATO common funded CIS Equipment is managed and safeguarded throughout the full materiel lifecycle process;
- CIS equipment, and CIS Spares and Consumables for a number of years of Integrated Logistic Support (ILS) of CIS Systems and Capabilities are available to support NATO operations, exercises, and the static infrastructure, with significantly reduced time between requisition and delivery;
- Improvement of the CIS Materiel Management and availability of stock managed items;
- The centralization of the codification, storage, warehousing, receipt, dispatch, transportation, and materiel coordination functions provides cost savings to the NATO Nations. This includes both NSIP as well as the follow on Operations and Maintenance activities;
- In cases where Spares supporting in-service systems are likely to become 'diminished manufacturing availability', they are procured, stored and available for supply by the CSSC Warehouse in order to ensure NATO Business Continuity;
- For no longer required equipment CSSC, if deemed re-useable, can provide suggestion for central storage, return to service or local dispose;
- Reduced overall costs per item managed through the stock management process.

Service Features:

- **Codification**: Codification and management of item master data information that is used to support procurement, supply and material management of CIS Equipment purchased using NATO common funding. Codification is used within NATO in order to improve CIS/Non-CIS identification, supply and property accounting. Codification, if carried out correctly, will result in cost savings for NATO as assets will be more efficiently and effectively managed in support of NCI Agency Service provision. The codification is also executed NCI Agency non-CIS equipment and common elements of the AMDC2 System in support of property accounting tasks. Codification is divided into Codification of CIS Assets and Codification of Non-CIS Assets.

- **Planning:** Planning, scheduling, coordination and documentation update for Storage Management and Warehousing Services. Planning, scheduling and coordination for Receipt and Dispatch Services. Planning, scheduling and coordination for asset management SME services.
- **Receipt/Dispatch:** The CSSC performs as the mainpoint of entry for the majority of new CIS equipment procured through common funding of NATO. The Receipt and Dispatch (R/D) activities are an essential element, which supports project execution, service delivery, supply management, asset management and database management activities associated with CIS. CSSC also receives and dispatches non-Common funded materials on request from some Host Nations and MoU organizations. The receiving process, which is managed in the ORACLE Inventory/Order Management database is handled either directly or indirectly by the CSSC Receipt and Dispatch. This is an Asset Management activity providing identification, serialization and traceability of CIS equipment. CIS Materiel consignments are processed, prepared and dispatched through the R/D section of CSSC. Dispatch can include freight forwarding, special deliveries, urgent request and courier coordination services. R/D also coordinates the most suitable and cost effective transportation service in conjunction with NSPA. Although NSPA is responsible for the management of transportation of CIS Material on behalf of the NCI Agency, CSSC provides a single point coordination Service to our internal and external customers to ensure that material moves are managed efficiently and effectively. Transportation Requests are received and processed by CSSC to support the original customer requests (MR/IR/MOI etc.). R/D also manages classified equipment.

- **Storage:** Assets are stored and managed in the CSSC Warehouse as part of the Inventory Project supporting the procurement, supply, exchange, repair and upgrade processes for CIS equipment within the NCI Agency. The Service relates to the CIS requisitioning and supply activities of the NCI Agency.

- **Stock Management:** CSSC provides a Stock Management Service in conjunction with the Inventory Project of the NCI Agency. Planning, scheduling, coordination and documentation update for stock management service. Supply of CIS stock managed materiel in line with PM requisition requirements. Replenishment activities related to all stock Managed CIS equipment.

- **SME Services**: Provide customers with near real time management of CIS Equipment Account Balances associated with the Custodian Account and Depot Stock Organization Structure. The inventory management service is an essential enabler of material management and property accountability. CSSC provides advice and support to the Operations and Exercise Service Line in the development of CIS Logistics related plans in relation to Exercise and Operational Planning. This planning effort may be dedicated to a specific Exercise/Operation or included within an existing SLA. CSSC provides expert logistics support to projects such as those related to the AMDC2 (AirC2/BMD) in the data capture and inventory setup/management of associated assets. CSSC conducts data cleansing activities in support of Projects/Programmes such as EBA and ITM. Although this is not meant to be a day-to-day activity, it is anticipated that this task will continue in excess of 12 months.

- **Inventory Management:** The indirect or direct support is provided to the Custodian Account holder in the completion of the annual inventory activities. The support activities are related to handling of discrepancies within an account balance list. This can be associated with the annual counting process or for an individual or multiple item loss/damage report.
- **Logistic Maintenance Support:** This is a required activity related to the accountability of CIS materiel that is returned by the customer for preventative or corrective maintenance actions or to storage for future reuse (reverse logistic). In these cases CSSC will conduct handover/takeover (HO/TO) checks of the property which includes full inventory of materiel prior and after completion of the maintenance activities.
- **End of Life asset management:** when an asset reaches his end of life (obsolescence, failure or loss), CSSC provides assistance in reporting, including pre-investigations, creation of Report Of Survey (ROS), in case physical handling of condemned equipment (palletizing, storage) and Write-off from the Book.
- **Support Planning** The HO/TO is an essential element of inventory checking when equipment is moved from the responsibility of one Sub-PAO to another or back to CSSC. The HO/TO process is required to ensure that common funded equipment is handled in accordance with the Financial Regulations and Asset Management Directives and Procedures.

Service Request: The Service may be requested in multiple ways:

- Identified within SLA / OLA;
- E-mail requests to Resource Management Branch Tasking Cell;
- EBA Project Management Milestone Request;
- EBA Internal Requisition;
- ITSM;
- EBA Work Request;
- EBA Move Order Transfer;
- EBA Internal Requisition;
- E-mail to Resource Management Branch Tasking Cell;
- Materiel Request through iProcurement.

Service Flavours: The Service is available in multiple flavours, depending on the required features and forms of support.

Available on: N/A

Service Prerequisites:

None

Standard Service Support Levels:

- **In House:** Equipment is stored, maintained and managed at the CSSC main warehouse and released and/or replenished on request from the relevant Service Line/Project Manager.
- **On Site:** Equipment is forward deployed to Buffer Stock locations in order to support the 'urgency' element of spares and consumable supply for Service Lines and PMs.
- **Routine:** Service provided as a routine process associated with standard timelines.
- **Urgent:** Service provided as a prioritized process associated with urgent requirements and timelines.
- **Codification**: All actions required for the execution and management of the codification will be conducted by the codification team within AMSB, CSSC.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

LOG002 Test Equipment & TEMPEST Level Testing

Service ID: LOG002

Service Name: Test Equipment & TEMPEST Level Testing

Service Type: Customer support

Portfolio Group: Engineering Services

Service Status: Available

Service Description: CIS Sustainment Support Centre (CSSC) Brunssum is NCI Agency single point of contact for all Test Equipment (TE) and Fibre Optic Reel (FOR) requirements, general maintenance, verification and repairs. This service entails initial acceptance testing of new procured TE and FOR, verification of calibration performed by external institutions, repairs and technical evaluation of items fulfilling manufacturer criteria to NATO standards. The service also entails equipment TEMPEST level testing to SDIP-27 standards under the technical direction of the NATO Cyber Security Centre (NCSC).

Value proposition: Conducting periodic maintenance and testing to ensure that all TE and FOR are safe to use, accurate to the original manufacturer's specifications, and traceable to back to international standards.

CSSC maintains the only TEMPEST facility within the NCI Agency conducting tests of commercial-off-the-shelf (COTS) CIS items used to process NATO CONFIDENTIAL and above.

Service Features:

- Testing and repair of TE and FOR to confirm manufacturer specification, performance and functionality.
- The periodic maintenance and testing of TE and FOR does not simply mean checking the specifications. A comprehensive function test and minor preventive maintenance are also performed, improving the reliability of the TE and preventing failures. At the same time, a firmware update will be performed to make sure the instrument has all the latest features.
- The standards used in the maintenance process are traceable to national and international standards or other intrinsic standards. The method and procedures used for certifying TE complies with most IEC/ISO 17025 and military requirements.
- All TE maintenance is performed either at the CSSC or at customer's location within a controlled environment room.
- Providing unbiased technical advice and engineering support, ensuring solutions are "fit for purpose" and "fit for use" whilst minimizing the cost to the customer.
- Performing mandatory Electrical Safety Inspection for compliance to NEN 3140 (standard for operation of electrical installations - Low voltage).
- Testing and evaluation of Electric Radiation (ER) signals for Compromising Emanation (CE) in order to allocate the appropriate SDIP-27 TEMPEST Level B or C rating.
- Acceptance testing of TEMPEST equipment certified by NATO Approved Suppliers to confirm that the equipment meets the SDIP-27 TEMPEST Level rating allocated.

Service Request: Assigning an ITSM ticket to CSSC Brunssum, technical support or via e-mail to the CSSC Resource Management Branch (RMB) who will coordinate internally to assess feasibility, required effort and personnel to be involved.

Service Flavors:

In-House support:

- TE and FOR will be maintained within the CSSC where additional shipping costs could arise.
- All devices to be TEMPEST tested need to be send to the CSSC.

On-Site support:

- Based on an accepted price proposal, TE and FOR will be maintained at customer location where additional transportation and staffing costs arise.

Available on: N/A

Service prerequisites:

- Operational Units have completed Level 1 and 2 maintenance activities including cleaning as laid down in the system maintenance guides.
- To ensure that battery operated TE are charged regularly.
- To provide access to any password protected hard drive.
- Operational Units have conducted a full inventory check of the system prior to the Handover Takeover (HO/TO) to the CSSC engineering and asset management teams to ensure that power supplies, batteries, and terminal connectors / adapters are included.
- Real Life Support provided at deployed locations to enable the conduct of the maintenance.

Standard Service support levels: N/A

Service Cost/ Price: The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

Categorized areas of measurement capability and types supported. Due to the huge variety of different models and build-in options, detailed costs will be provided to customers on a case-by-case. Cost in TAS hours seen in table below, is indicative average cost per item.

	Type of Test Equipment	Support	Average Costs
Category A	RF attenuator set / step, termination, power splitter / divider, directional coupler, high power load, optical sources, power meter, attenuator, optical laser source, fusion splicer, cable analyser, smart remote, LAN tester, digital multimeter (hand held), clamp on meter, high voltage probe, ISDN tester, bit error rate tester, RF power sensor, sweep generator, frequency counter, radiation meter and field probe, 8,5 digit bench multimeter, oscilloscope (Hand Held), megger, cable tester, data communication analyser, media test set ...	TE In-house Onsite	Average TAS hours 1.5, which could deviate depending of the model to be tested.
Category B	OTDR modules, spectrum analyser (hand held), oscilloscope, earth ground tester, communication analyser, function generator, test set analyser…	TE In-house Onsite	Average TAS hours 3.0, which could deviate depending of the model and options installed.
Category C	RF signal generator, level generator, OTDR (hand held), …	TE In-house Onsite	Average TAS hours 5.0, which could deviate depending of the model and options installed.
Category D	OTDR bench type (quad models), precision spectrum analyser, ATM tester, network analyser, signal analyser…	TE In-house Onsite	Average TAS hours 8.0, which could deviate depending of the model and options installed.
Category E	Repair of fibre optic cable reel and testing (e.g. 500m, Type HMA connector, Single Mode)	FOR In-house	Average TAS hours 3.0, which could deviate depending of the type, and installed connectors.

	Type of TEMPEST Equipment	Support	Average Costs
Category A	Keyboard, smartcard readers, …	TEMPEST In-house	Average TAS hours 0.5, which could deviate depending of the model to be tested.

Category B	Ext. DVD writer, monitor, TFT, KVM, switch, router, VoIP Phone, tablet, firewall, ...	TEMPEST In-house	Average TAS hours 2.0, which could deviate depending of the model and options installed.
Category C	Server, scanner, PC, projector, Thin Client, beamer, printer, …	TEMPEST In-house	Average TAS hours 2.5, which could deviate depending of the model and options installed.
Category D	Video Teleconference (VTC), Laptop …	TEMPEST In-house	Average TAS hours 4.0, which could deviate depending of the model and options installed.

LOG003 Test and Evaluation of Electromagnetic Environmental Effects Service – 3rd Level

Service ID: LOG003

Service Name: Test and Evaluation of Electromagnetic Environmental Effects Service – 3rd Level

Portfolio Group: Logistic Services

Service Description: The Service entails Shielding Effectiveness Testing and maintenance of shielded enclosures to meet the requirements for Electromagnetic Pulse Protection (EMPP), Communication Security (COMSEC), TEMPEST and any other Radio Frequency (RF) interference protection on NATO common static facilities and transportable CIS systems according to MIL-STD-188 125-1/2 and SDIP 29/2. Testing is performed on all NATO shielded enclosures and bunkers, detailed in the ACO Directive 80-052 and all NATO mobile Communications and Information Systems (CIS) embedded in shelters or transportable boxes particularly used with CP0149 at various locations and mission related systems in Resolute Support (RS).

Value proposition: Regular inspections / maintenance are required to assure the required Radio Frequency (RF) shielding for all NATO common funded facilities, installations, and CIS (ACE Manual 93-5-1). Inspection serves the purpose to determine whether the facilities, installations and CIS are protected for EMP, COMSEC and TEMPEST. Testing, in accordance with the equivalent standards and the use of associated reference documentation, is the mandated method of managing the risk of damages caused by electromagnetic pulse and of avoiding the capturing and re-transmitting of NATO classified information.

Service Features:

- Planning, scheduling and coordination for electromagnetic environmental effects (E3) service
- Subject Matter Expertise (SME) in RF measurements of attenuation provided by the shield (Shielding Effectiveness [SE] testing) according to the IEEE STD-299, as well on existing and new up-coming projects with E3 concerns
- Testing of:
  - RF Shielded Enclosures
  - TEMPEST Testing Facilities
  - Microwave Sites
  - Satellite Ground Terminal (SGT)
  - Satellite Ground Segment (SGS)
  - CIS Systems (TSGT 2nd &TSGT 3rd Generation; SRDLOS; LRDLOS)
  - CIS Shelters (HF; Crypto; Helpdesk; AirC2; SIGINT COINS; NNCCRS)
- EMPP testing of Bunkers as detailed in the Allied Command Operation (ACO) Directive 80-5
- Annual inspection and preventive maintenance according to Allied Command Europe (ACE) Manual 93-5-1

- Testing of power and signal line filters according to MIL-STD-220 and publication method CISPR17
- Maintenance on manual and pneumatic operated electromagnetic shielded doors
- Acceptance testing of new and modified installations
- Technical advice of lightning, surge protection and grounding of CIS networks including power distribution systems
- Analysis and technical advice related to Electromagnetic Field Safety (EMF) of workplaces imposed by European and derived National Regulations

Service Flavors:

- **On-Site Support**: testing and measurements performed at the customer's site.

Available on: N/A

Service prerequisites: None

Standard Service support levels: N/A

Service Cost/ Price: Service Cost / Price: The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

LOG004 Inspection of Electronic Devices for Security Measures

Service ID: LOG004

Service Name: Inspection of electronic devices for security measures

Portfolio Group: Logistic Services

Service Description: The Service entails measurement of extremely low-level RF emanating signals of electrical devices. Within a shielded enclosure, isolated from external RF environmental noise, the RF energy of activated devices can be detected and reported across a wide frequency band. This could be used for individual devices, smaller than 80cm width, up to a system of components.

Value Proposition: Physical and technical inspection of equipment is essential to mitigate the threats associated with the unauthorized implantation of devices, substitution of equipment or manipulation of functionality within electronic equipment to achieve an eavesdropping capability. Without this initial inspection, electronic equipment is not readily possible to determine whether or not the equipment is “fit for purpose” and more importantly, whether or not it is “secure”. The level of security being directly correlated to whether or not such equipment contains any embedded malware and / or eavesdropping devices that can be exploited to capture and re-transmit NATO classified information.

Service Features:

- **Active testing technique:** undertaken by actively stimulating the equipment (i.e. simulating the processing of information).
- **Passive testing technique:** listening to the equipment’s electronic operation to detect any unusual or unexplained functionality, emanated signals and/or frequencies.
- **Shielded enclosure testing** for bugs, excessive Radio Frequencies (RF) emissions at frequencies around GSM 3G/4G and Wifi. Evaluation of Emanating Radiation (ER) for compromising emanation.
- **Analysis** of the effects of broadcasting audio signals
- **24h test** to look for transmissions of signals without any stimulus.

Service Flavors: The service is offered as a single flavour:

> In-House support: all devices to be tested need to be send to the CSSC where additional shipping costs could arise.

Available on: N/A

Service Prerequisites: None

Standard Service Support Levels*:* N/A

Service Cost / Price: The unit of measure is per testing. Provided the variety of possible device and enclosure testing, each testing is costed specifically.

LOG005 Support to Exercises with Deployable CIS Equipment Pool (DCEP) Service

Service ID: LOG005

Service Name: Support to Exercises with Deployable CIS Equipment Pool (DCEP) Service

Portfolio Group: Logistic Services

Service Description: The Service provides CIS user equipment from a DCEP Pool to eligible customers in order to support the exercise requirements of the Allied Command Operations (ACO). The service comprises: planning and coordination activities to make sure that high level exercise support requirements are matched with technical capability and existing capacity of DCEP; asset management and supply (including arranging transportation), maintenance (bench check, cleaning and serviceability testing) as well as logistics maintenance support of the DCEP pool.
The pool contains laptops, workstations, telephones, printers, projectors, Video Teleconference (VTC) Terminals, Multi-Function Devices (MFD), and LAN extension assets to expand the user access domains for each flavour of the DCIS node (in accordance with INF020 service definition).
The service does not comprise: build, upgrade, repair of DCEP pool assets (covered by INF020), on-site support and support to customer funded exercises (covered by specific Exercise Budget), upgrade (major configuration changes covered by NSIP projects). Costs of commercial shipments are charged against respective exercises.

Value Proposition: Centralization of the DCEP pool at CIS Sustainment Support Centre (CSSC) enabling smooth and coordinated CIS user equipment distribution to customers in support of the exercise requirements of the Allied Command Operations (ACO).

Service Features: Support to Exercises with Deployable CIS Equipment Pool (DCEP) Service provides planning and coordination, logistics as well as maintenance activities.

- **Planning and Coordination:** In coordination with NCIA Operations and Exercises Service Line (OPEX), appropriate CSSC representation is present at key planning events in order to provide right level expertise required to evaluate feasibility of requirements' fulfilment and coordination of proceedings leading to the provision of service at a required level. Resource Management Branch (RMB) leads this process. Upon receipt of the DCEP requirements, CSSC analyses them by performing quantitative and qualitative checks as well as, together with ACO J6 CyOC and NCISG, de-conflicting delivery dates for the customer locations. CSSC receives requirements from OPEX according to the timelines based on ACO exercise planning process.
  As in INF020 service, Service Delivery Schedule and Change Management Plan as planning and coordination tools are used and updated on a monthly basis. Service Delivery Managers (SDM) also provide Service Availability Management and Service Obsolescence Management Reports.

- **Logistics:**

o **Storage:** Most of DCEP assets are stored in sturdy cases allowing multiple deployments without too quick degradation of equipment. After DCEP is received back from exercise and cleaning, bench check test, serviceability check (maintenance activities) are accomplished, equipment is put back each time into cases making preparation time for next deployments shorter.
o **Dispatch:** After CSSC internal task is released, respective asset management activities are performed and the warehouse team (cleanliness, serviceability check), along with the crypto custodians as required, prepare consignments to be dispatched to the customer. Receipt and Dispatch (R&D) team coordinates and tracks deliveries, as per requested timelines. Equipment can be collected or shipped commercially, as per requirements/possibilities. Shipping is not included in the service rate.
o **Receipt:** Upon completion of the exercise, the DCEP is returned, in its entirety to the R&D and inventoried within 24 hours of physical receipt. As discrepancies are identified, the R&D reports the information to the RMB for rectification.
o **Logistics Maintenance Coordination (LMC):** Equipment returned from exercises is processed to respective workshops and according to particular types of equipment for serviceability test (e.g.: motherboard, memory, processor, network card, video card, storage, battery, usb).

• **Maintenance:** The various workshops of the Engineering and Maintenance Branch (EMB) perform full serviceability check of received equipment. After bench checking all serviceable assets are sent back to storage. If unserviceable items are identified, they will be processed for repair at CSSC or sent for an external repair. Note: The repair itself is excluded from this service as included in INF020.

Service Flavours: The Service is available as a single flavour.

Available on: N/A

Service Prerequisites: DCEP capability is provided by service INF020.

Standard Service Support Levels:

- **In House:** Equipment is stored, maintained and managed at the CSSC main warehouse and received and/or issued on request.
- **Routine:** Service provided as a routine process associated with standard timelines.
- **Urgent:** Service provided as a prioritized process associated with urgent requirements and time-lines.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

This page is left blank intentionally

Other Services

This page is left blank intentionally

OTH002 Account Management Service

Service ID: OTH002

Service Name: Account Management Service

Portfolio Group: Other Services

Service Description: The Account Management Service provides dedicated Account Managers to each NCI Agency eligible customer. Account Manager (AM) is responsible for Customer engagement, and establishes and maintains the Agency relationships with a customer or group of customers. AM serves as the principal interface between the Customer and the delivery of the NCI Agency services, ensuring understanding of the Customer's demands and their translation into clear set of requirements for services, as well as in sound plans how to meet these demands.

This service is provided as part of the established/signed service agreement. Accordingly, service cannot be requested separately, i.e. without the existence of an agreement.

This service only includes the Agency's centralised activities and resources required for service delivery. Local support from collocated staff in support of Account Management, Customer Relationship and Service Level Management daily operations is not included, and must be funded locally.

Value proposition: The Service provides a principal focus and entry point into the Agency for routine CIS services business. It enables clear establishment of requirements and ensures more effective service delivery monitoring and feedback, thus supporting overall efficiency and effectiveness in meeting Customer's CIS services demands.

Service Features:

Customer relationship management: the Account Manager (AM) provides focal POC for the Customer in the NCI Agency regarding CIS services, and understands Customer's business/operational processes and how NCI Agency CIS services may support them. He/she ensures Customer CIS services requirements are properly understood within the NCI Agency and represents Customers' interests within internal NCI Agency processes of prioritization and service delivery. AM maintains relevant information on the Customer required for internal NCI Agency business processes and streamlines interaction between different organisational levels of the NCI Agency and the Customer. AM enables effective Customer's definition of CIS service requirements and identifies any relevant new opportunities for improvements of the relationship between NCI Agency and its customers.

Customer request management: AM receives customer requests and subsequently manages the prioritisation of this request through the Agency Business Intake process, communicating as appropriate to keep the Customer fully informed.

Development, coordination and amendment of service provisioning agreements: AM is the Customer and Agency focal point for tracking the production, issue and acceptance of formal offers from the Agency for any service delivery (Service Level Agreements, Service Support Packages, etc.).

Complaint and escalation Management: AM coordinates internal NCI Agency management of any problem the Customer may have in relation to the NCI Agency delivery of services and ensures prompt feedback to the Customer on the progress.

Reporting: AM contributes to reporting on service provisioning in accordance with specific stipulations established within service provisioning agreements.

Service Flavours: The Service is available in following flavours:

Account Management of the Global Enterprise Centralized Service Level Agreement (CSLA): provides AM service to a customer having a large, consolidated service level agreement with NCI Agency for provision of the CIS services across entire NATO CIS enterprise. Applicable only to the Centralized Service Level Agreement.

Account Management of an Enterprise Service Level Agreement (ESLA): provides AM service to customer(s) having a consolidated service level agreement with NCI Agency for provision of CIS services to multiple user organizations customers tied into one organizational and/or budget structure.

Account Management of a Local Service Level Agreement (SLA): provides AM service to customers having a service agreement with NCI Agency for provision of CIS services to a single user organization (which may have elements of other user organizations as additional elements within the same SLA).

Account Management of a Service Support Package (SSP): provides AM service to customers having a Service Support Package with NCI Agency for provision of CIS services.

Available on: N/A

Service Prerequisites: None

Standard Service Support Levels*:* N/A

Service Cost / Price: The unit of measure for the Service is Per Agreement. For the price details, see the Service Rates document.

OTH003 AirC2 In Service Support Program of Work (ISS POW) General Support Service

Service ID: OTH003

Service Name: AirC2 In Service Support Program of Work (ISS POW) General Support Service

Portfolio Group: Other Services

Service Description: The Service entails services provided to ACO as a part of the AirC2 ISS POW that are not directly related to individual application services, due to the generic nature of performed activities to support services across a number of systems.

Value proposition: The service enables the overall delivery of the in-service-support for a number of applications and systems in support of the NATO Integrated Air and Missile Defence System (NATINAMDS).

Service Features: The service entails the following activities:

- Contract and licence management;
- Interoperability management;
- Security management;
- Support to AirC2 governance meetings and related NATO committees and Working Groups;
- Support to enabling Platforms and Tools;
- Development of POW related price proposals and requirements documents.

Service Flavours: The Service is available as a single flavour.

Available on: N/A

Service Prerequisites:

None

Standard Service Support Levels: N/A

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

OTH004 DCIS – Management Support Service

Service ID: OTH004

Service Name: DCIS – Management Support Service

Portfolio Group: Other Services

Service Description: The Service provides Operations Planning and Service Management (OPSM) support to the customer, as well as the primary NCI Agency interface and initial point of contact with the customer for in year execution of the services in accordance with agreed standards within the Service Level Agreement (SLA). The Service entails the management and coordination of all Deployable Services that are delivered to the service consumer at each of their peace time locations.

Value proposition: The Service provides management and reporting of all services, providing confidence to the customer that services delivery will continue as described in the respective SLA.

Service Features: The Service has the following features:

- Service monitoring, measuring, and Quality reporting, as defined in the SLA including Quarterly Service Level Reports;
- Availability Management Quarterly Service level Report (QSLR);
- Change Management Plan, Monthly update;
- Obsolescence Management, Quarterly Report on End of Life (EoL) of software and/or hardware;
- Service Delivery Schedule (Mid-Term and Short-Term Planning and coordination of Preventive Maintenance Activities (PMI), Advanced Schedule Interventions (ASIs), and Minor and agreed Major Changes);
- Transition Management for projects that are in support of the customer, but funded through the NATO Security and Investment Program (NSIP);
- Customer Account Management to supplement, but not replace, existing processes, for example: Customer Request Form (CRF) and related Price Proposal/ Purchase Order tracking, Exercise/ Operational planning, SLA Development, etc.
- Completion reports after each scheduled maintenance activity.

Service Flavours: The Service is available as a single flavour.

Available on: N/A

Service prerequisites: None

Standard Service Support Levels: N/A

Service Cost / Price: The Service is costed as an underlying service within each DCIS service (INF020, INF035, INF036, INF037, INF040, INF044).

OTH005 Training Capability Battle Lab Support Service

Service ID: OTH005

Service Name: Training Capability Battle Lab Support Service

Portfolio Group: Other Services

Service Description: The Training Capability Battle Lab Support Service provides CIS services*[1] and expertise in the Modelling and Simulation (M&S), Training and Exercise (T&E), and CIS expertise required to support planning, design, management, and execution of the customer's Training Capability Battle Lab's annual program of work for testing, experimentation, capability development and wargaming in support of Warfare Development.

Caveats:

- The service assumes that the security accreditation and the operational use of the Training Capability Battle Lab are responsibilities of the customer.
- The service provides O&M of one unclassified platform.
- The service is currently designed for the JFTC environment and to meet JFTC's requirements.

*[1] *Disclaimer: The IT platform and services are provided locally and will need to be modified to be ITM compliant after ITM delivers to the sites where this platform is used.*

Value Proposition: The service supports:

1. Testing, experimentation and concept development requirements based on a combination of existing and/or new M&S, T&E, and interoperable capabilities of NATO, Allies, Partner Nations, and Industry.
2. Wargaming requirements based on existing NATO Modelling and Simulation capabilities with validated data sets replicating multi-operational domain warfare environment.

Service Features:

The service provides the following:

1. Management of a platform, including a combination of existing and/or new M&S, T&E and interoperable capabilities of NATO on the Battle Lab Unclassified standalone platform with VPN connectivity.
2. A combination of existing and/or new T&E and/or interoperable capabilities of NATO on the following existing platforms:
   - CFBLNet Pink,
   - CFBLNet Grey,
   - Exercise MS.
3. Existing NATO T&E capabilities with support for validation of data sets replicating multi-operational domain warfare environment on the existing Exercise MS platform.
4. Best-effort CIS support on the existing Battle Lab Standalone unmanaged platform that consists of laptops with OS connected to a standalone LAN.

5. The required flexibility, enabled by providing:
   a) Standing capabilities on supported platforms with a pre-defined set of systems and their interconnections;
   b) Pro-active maintenance to prevent issues and manage availability;
   c) Managed roadmap for systems to ensure agreed versions of systems are available and operational;
   d) 10% capacity to add new capabilities or new versions of capabilities;
   e) Dedicated on-site support by a team of CIS staff integrated with the customers' Battle Lab event management team;
   f) A set of pre-approved standard service requests with defined standard service fulfilment times;
   g) Critical priority response and restoration times (P1) during Training Capability Battle Lab event execution or as agreed in the event planning phase;
   h) Remote connections for remote support purposes;
   i) Remote connections for 3rd party users;
   j) Provisions for on-boarding of non-AFPL listed systems and users.

Service Flavours: The Service is available as a single flavour.

Available on: NU Standalone, MS (Exercise NS), CFBLNet Pink, CFBLNet Gray

Service Prerequisites: This service is a combination of SME services and locally provided CIS services on the existing platforms, limited to MS, CFBLNet networks, and Battle Lab Unclassified Standalone. In principle, the locally provided services are provided based on (where available) or in line with the existing services provided by NCI Agency. The service assumes that the required target platforms are not part of the service and that they are already available.

Standard Service Support Levels:

Service Time Window	Priority
Planned event execution • **pre-approved service requests**	P1 – Critical During business hours in working days
Planned event execution • **other service requests**	P3 During business hours in working days
Regular (outside planned events), including event planning, preparation and tear-down	P3 During business hours in working days

Service Availability Target:

- Downtimes for maintenance - number of allowed downtimes: 1 per month, pre-notification periods: 2 weeks, max downtime time pre system: 2 working days
- Maximum service usage time without maintenance: 1 month

- Interruptions to the Service (both planned and unplanned) will be coordinated with the Customers' Battle Lab manager

Service Restoration:

Priority	Time to Respond (Incident or Service Request)	Time to Restore (Incidents)
P1 – Critical **During business hours in working days**	1 h wall clock	4 h wall clock
P3 **During business hours in working days**	8 h business hours or 1 working day	16 Business hours or 2 working days

N.B. Full Priority Resolution Times and Generic Service Priority Assignment Matrix will be adhered to in accordance with the NCI Agency standardised SLA.

Service Cost / Price: The unit of measure for the Service is 1. The total of the Service delivery cost is charged in accordance with specifically arranged conditions of the Service delivery.

NATO
OTAN
NATO Communications and Information Agency
NCI AGENCY

NATO Digital Workplace Services

NDW001 NATO Digital Workplace Service (Low Side)

Service ID: NDW001

Service Name: NATO Digital Workplace Service (Low Side)

Portfolio Group: NATO Digital Workplace Services

Service Status: Pipeline

Service Description: The brand new NATO Digital Workplace Service is the future work environment for NATO staff. NDW001 features all the features and functionality required in NATO's Digital Workplace including computing platform, content creation features and access to a wide range of content collaboration platforms available.

NDW001 not only simplifies the standard service offerings but also unites the NATO Enterprise by ensuring that previously fragmented features and functionality are made available to all NATO Enterprise staff through global availability of tools and software in the NATO Digital Toolbox.

NDW001 provides the environment so staff can connect, communicate and collaborate in an effective way taking Staff Productivity and Enablement to the next level.

Value Proposition: Previously, a lengthy set of Workplace Services were required before a staff members were able to perform their duties. With NDW001 a comprehensive set of features and functionality are provided by default as one cohesive intelligence in order to unite the NATO Enterprise.

The initiative is part of the Office of the NATO CIO (OCIO) championed near-term initiatives[1] providing the Digital Workplace 2.0. The creation of NDW001 is in direct support of NATO's Digital Transformation Vision achieving a Digital Workforce. The Digital Workplace is an integrated part of the NATO Enterprise Digital Transformation Action Plan and is located under the Digital Enablement part of the Technology Pillar (together with the Digital Backbone and Cloud Services initiatives).

Service Types: NATO Digital Workplace Service (Low Side) service types:

NDW001 comes only in one service type which is covering the low side (NU/NR). The equivalent service for higher content classification can be found under NDW002 NATO Digital Workplace Service (High Side)

Service Features: The Service provides the following minimum features:

- Computing Platform (Operating System) depending on the selected hardware (NDW003)
- NCN telephone extension number*
- Commercial telephone number*
- Workstream Collaboration features
- Digital Signature (NATO PKI certificate)
- Hardware authentication token

[1] OCIO(2023)0122, NATO Digital Workplace (NDW) Workshop Report, dated 5 June 2023 refers

- Enterprise Managed Mobility
- Content Creation features (Microsoft Office Professional, Adobe Reader)
- Unified NATO identity (@ENTITY.nato.int or @nato.int)
- Personal Storage Space
- Digital #OneNATO name (ENTITY | LASTNAME Firstname | *Optional Fields*)
- Social Platform (ME)
- Access to NATO Enterprise Intranet Packaged Platform
- Access to socialisation content (training material, videos, etc.)
- User support (based on support hours selected)**
- Mandatory Security Components
- Life-Cycle Management of Enterprise Candidate Applications
- Device Management (patching etc.)

***Note**: feature might not be available in selected entities due to missing underlying capabilities, local leadership decisions or other external factors

****Note:** Please see Standard Service Support Levels below for support options

Available on:

Service Type	Stand Alone Device*	NATO Unclassified CIS*	NATO Restricted CIS*	NATO Secret CIS*	Mission Secret CIS*
NDW001	✓	✓	✓		
NDW002				✓	✓

*** NDW001 is only available on NCI Agency support CISs (for example NU PAN, REACH, MAGELLAN etc.**

Service pre-requisites:

NDW003 Hybrid Work Environment - Managed Device Service

- One or more devices are required as per compatibility matrix below

WPS003 Enterprise User License Service*

- WPS003-1 Standard User, or
- WPS003-2 Light User

*** Note:** From a licensing perspective a maximum of two devices (WPS003-2 Light User) or five devices (WPS003-1 Standard User) is supported. It is a user responsibility to ensure that the maximum number of devices assigned is not exceeded.

Service Type	Device supported by NDW001	Remarks

NDW007-A Static Desktop (Workstation) Device	✓	Limited feature set
NDW007-B Thin Client Device	✓	Requires supporting Virtual Desktop Infrastructure (VDI) backend to be present
NDW007-C Portable (Laptop) Device	✓	
NDW007-D SECUNET Client (Multi-Domain Client) Device	✓	Each low-side session hosted on the multi-domain client requires separate instance of NDW001
NDW007-E INTEGRITY Client (EAL-6 certified Multi-Domain Client) Device	✓	Each low-side session hosted on the multi-domain client requires separate instance of NDW001
NDW007-S Smartphone/Tablet (iOS device only)	✓	Selected feature set only

Standard service support levels:

Service Availability:

The NDW001 NATO Digital Workplace Service is expected to be fully functional 24/7*. In the unlikely event any issues related to the service needs to be reported the service support hours available are:

- Standard Support: 08:30 - 17:00 (included in standard service rate)
- VIP Support: 06:00 - 22:00 (service rate available upon request)
- VVIP Support: 00:00 - 23:59 (i.e. 24/7 support) (service rate available upon request)

* Only if one of the following conditions are met, the service will be considered unavailable:

1. Single or multiple features are unavailable to minimum all users in an organisation. For example users are unable to sign document digitally, or the entire NPKI capability is unavailable.

Service Restoration:

Service availability target is 24/7 availability with Priority Resolution Times and Generic Service Priority Assignment Matrix in accordance with the NCI Agency standardised Service Level Agreements in force, for example ABIPAT.

- **Service Quality level 1:** Service Restoration within 4 hours
- **Service Quality level 2:** Device replacement on request with no guaranteed service restoration time

Service Reporting:

Quarterly Reports:

Based on final outsourced contract but expected to include:

- Quantity of NDW001 instantiated at each geographical location
- Quantity of NDW001 instantiated on devices that has reached life expectancy
- Number of incidents raised per feature

Service Cost / Price:

The unit of measure for the service is per user and includes mandatory security software (if applicable), licenses and subscriptions plus standard accessories such as keyboard, mouse, etc.

The number of Service Units will be determined based on active user accounts on the respective CIS where the NDW001 NATO Digital Workplace Service is utilized.

Service initiation:

For customers who are procuring new quantities of the service, the service initiation rate (procurement and deployment of the service components) shall apply as a one-time cost.

Please see ANNEX 1 for the detailed service initiation rate.

Instantiation time for new unit is 8 business hours depending on availability of dependent services, i.e. WPS003 Enterprise User License Service and NDW003 Hybrid Work Environment - Managed Device Service.

Annex 1

Service	Device	Service Initiation SSC (EUR)	Remarks
NDW001 NATO Digital Workplace Service	Any NDW001 supported Device (NDW003) Service Type	TBD	

Annex 2

Feature	Previously included/provided by	Native feature in NDW001	Remarks
Computing Platform (Operating System)	WPS001, WPS016-A	✓	
NCN telephone extension number	WPS009	✓	
Commercial telephone number	Limited availability	See remarks	Standard feature in NDW001. However, feature might not be available in selected entities due to missing underlying capabilities, local leadership decisions or other external factors
Workstream Collaboration features	WPS012	✓	
Digital Signature (NATO PKI certificate)	÷	✓	New feature
Hardware authentication token	WPS016-C	✓	
Enterprise Managed Mobility	WPS016-C	✓	
Content Creation features (Microsoft Office Professional, Adobe Reader)	WPS001	✓	
Unified NATO identity	WPS002 (limited support)	✓	
Personal Storage Space	WPS002	✓	Default allocation: 20GB/user

Digital #OneNATO name	÷	✓	New feature
Social Platform (ME)	WPS006 (NR AIS only)	✓	
Access to NATO Enterprise Intranet Packaged Platform	÷	✓	New feature
Access to socialisation content (training material, videos, etc.)	÷	✓	New feature
User support (based on support hours selected)**	WPS008	✓ (extended options)	
Mandatory Security Components	WPS001, WPS016-C	✓	
Life-Cycle Management of Enterprise Candidate Applications	÷	✓	New feature
Device Management (patching etc.)	WPS001, WPS016-C	✓	

NDW003 Hybrid Work Environment – Managed Device Service

Service ID: NDW003

Service Name: Hybrid Work Environment - Managed Device Service

Portfolio Group: NATO Digital Workplace Services

Service Status: Pipeline

Service Description: The Hybrid Work Environment - Managed Device Service provides users with various physical devices, that allow~~s~~ them to utilize the NDW001/NDW002 NATO Digital Workplace Services or other Application Services which require a physical device in order to secure a connection to NATO networks (in a specific security domain).

The Hybrid Work Environment - Managed Device Service includes commodity devices such as workstations, laptops, thin clients, smartphone/tablets, desk phones and other devices required to create an effective digital workplace. The service includes as a minimum an operating system or specific firmware required to achieve the stated service quality. Additionally, the service includes mandatory security tools, accessories, licenses and subscriptions required to maintain the service quality of the device.
The Hybrid Work Environment - Managed Device Service excludes automatic procurement of new devices when they have reached their life expectancy. Similarly, the service excludes the cost life-cycle replacement of obsolete equipment.

Value Proposition: The service offers a managed device enabling users to perform their duties in an effective and consistent way. It is closely linked to the NDW001/NDW002 NATO Digital Workplace Services which provides the comprehensive Digital Workplace experience at both Low Side (NU/NR level) and High Side (NS level), ensuring operational efficiency and effectiveness throughout the NATO Enterprise.

The Hybrid Work Environment - Managed Device Service ensures active obsolescence management can be provided, i.e. that the customers have an always accurate overview of their devices (assets) and their associated life-expectancy enabling entities to proactively plan and budget for life-cycle replacement.

Service Types. The Hybrid Work Environment - Managed Device Service service types:

> **NDW003-A Static Desktop (Workstation) Device -** This device is a workstation that needs to be connected to a wired network. It features a keyboard and mouse. In exceptional cases, a Static Desktop Device may be provided as a standalone device. Monitors are *not* included in the service type and needs to be selected in the quantities required through the NDW003-M service. A total of three monitors can be connected by default.
>
> > **Note:** Static Desktop Devices are no longer used at Low Side (NU/NR level) unless required by specific performance based applications. For standard Low Side usage, please see NDW003-C Portable (Laptop) Device service type.

NDW003-B Thin Client Device - This device is a computing device that runs from resources stored on a central server instead of a local hard drive, commonly referenced to as a Virtual Desktop Infrastructure (VDI) device. Thin clients work by connecting remotely to a server-based computing environment where most applications, sensitive data and memory are stored with the need to be connected to a wired network. Monitors are *not* included in the service type and needs to be selected in the quantities required through the NDW003-M service. A total of two (TBC) monitors can be connected per default.

NDW003-C Portable (Laptop) Device - This device can either operate as stand-alone device, be connected to a wired network or connected to a wireless network. It comes with an external power adaptor and protective sleeve by default. All other accessories shall be ordered separately.

Note: The NDW003-C Portable (Laptop) Device, can be connected to NCI Agency supported CIS through various connectivity:

- Static connection, i.e. cabled connection to an existing low-side or high-side network (high-side requires Wifi and cellular disabled)
- Remotely through either WiFi or cellular connectivity (low-side only).

Note: Tablets running Microsoft Windows Operating system will be considered under NDW003-C service type.

NDW003-D SECUNET Client (Multi-Domain Client) Device - This device (laptop) features a Multi-Domain capability, i.e. the device can connect to multiple systems running at different content classification levels (for example NU and NR) or systems operating at same content classification level but with different service providers (for example NR and NR *or* NATO CIS and National CIS) [1].

Note: This service type is only available for customers who have the supporting backend infrastructure implemented (subject to separate funding agreement).

NDW003-E INTEGRITY Client (EAL-6 certified Multi-Domain Client) Device - This EAL-6 certified device (laptop) features a Multi-Domain capability, i.e. the device can connect to multiple systems running at different content classification levels (for example NU and NR) or systems operating at same content classification level but with different service providers (for example NR and NR *or* NATO CIS and National CIS) [2].

Note: This service type is only available for customers who have the supporting backend infrastructure implemented (subject to separate funding agreement).

NDW003-S Smartphone/Tablet (iOS device only) - this service type accounts for an Apple iPhone/iPad device including its associated management configuration ensuring the device is in compliance with applicable cyber security configuration (Mobile Device Management (MDM) configuration). It comes per default with an external power adaptor, authorized

[1] Subject to standard security accreditation and security approval activities

[2] Subject to standard security accreditation and security approval activities

Bluetooth headset (Apple AirPods), protective cover and screen protector by default. Tablets will have a protective cover with embedded keyboard and Apple Pen by default.

DW003-M Monitors - This service type covers all types of monitors (display systems) that are connected to other NDW003 service types or which are used in conjunction with the NDW003 Hybrid Workplace (Audio/Visual Services). The service type covers all screen sizes available in the NCI Agency's procurement catalogue.

NDW003-P Voice over Internet Protocol (IP) phone - This service type accounts for a physical Voice over IP (VOIP) device used on both Low Side (NU/NR) and High Side (NS/MS). The device comes with mandatory cyber security components and required software/licenses.

Available on:

Service Type	Stand Alone Device	NATO Unclassified	NATO Restricted	NATO Secret*	Mission Secret*
NDW003-A	÷ **See note 1**	÷ **See note 1**	÷ **See note 1**	✓	✓
NDW003-B	÷	✓	✓	✓	✓
NDW003-C	✓	✓	✓	✓ **See note 2**	✓ **See note 2**
NDW003-D	÷	✓ **See note 3**	✓ **See note 3**	✓ **See note 4**	✓ **See note 4**
NDW003-E	÷	✓ **See note 3**	✓ **See note 3**	✓ **See note 4**	✓ **See note 4**
NDW003-S	✓	✓	✓	÷	÷
NDW003-M	✓	✓	✓	✓	✓
NDW003-P	✓	✓	✓	✓	✓

*** TEMPEST testing of devices used on High Side (NS/MS) is mandatory**

Note 1: Supported if required by specific performance based applications

Note 2: Requires supporting Virtual Desktop Infrastructure (VDI) backend to be present

Note 3: Requires supporting backend infrastructure implemented (subject to separate funding agreement)

Note 4: Requires supporting backend infrastructure implemented (subject to separate funding agreement), for example NS Mobility service.

Please note: For devices used on the high-side (NS/MS), TEMPEST testing of each devices is mandatory. The cost for TEMPEST testing is a one-time only cost which will be included in the Service Initiation cost. The Annual Service rate for both TEMPEST and non-TEMPEST tested devices remains the same.

Service pre-requisites:

INF001 LAN Service (not applicable to standalone devices)

Service lifecycle for devices: The below table shows life expectancy per device category , the service owner shall inform the entity utilising the device before life expectancy reaches within a suitable time frame.

Service Component	**Life Expectancy**
NDW003-A Static Desktop (Workstation) Device	5 Years
NDW003-B Thin Client Device	6 years
NDW003-C Portable (Laptop) Device	3 Years
NDW003-M Monitors	5 Years
NDW003-S Smartphone/Tablet (iOS device only)	3 Years
NDW003-P Voice over Internet Protocol (IP) phone	7 Years

Standard service support levels:

Service Availability:

The devices are expected to be fully functional 24/7 throughout their life expectancy and therefore only procured with the minimum standard limited warranty period as per national regulations in country of procurement (for NCI Agency procured devices this is normally Kingdom of Belgium).

Please note that it is not possible to procure additional warranty period for NDW001 Hybrid Work Environment - Managed Workplace Devices as NATO has implemented a “discard model” where faulty devices will be replaced instead of intended for repair.

Service Restoration: Where the device is deemed faulty, the service restoration period will be 4 hours for locations with on-site spare devices. For all other locations, service restoration period is based on the procurement/shipping time for replacement devices.

- **Service Quality level 1:** Service Restoration within 4 hours
- **Service Quality level 2:** Device replacement on request with no guaranteed service restoration time

Service Reporting:

Quarterly Reports:

Based on final outsourced contract but expected to include:

- Number of Service Types at each geographical location
- Service Type lifetime against life expectancy

- Number of incidents raised per Service Type
- Number of faulty Service Types replaced
- Recommended life-cycle replacements within next 12-18 months (only until life-cycle replacement is included in service rates)

Service Cost / Price:

The unit of measure for the service is per device and includes mandatory security software (if applicable), licenses and subscriptions plus standard accessories such as keyboard, mouse, etc.

Service initiation cost:

For customers who are procuring new quantities of the service, the service initiation rate (procurement and deployment of the service components) shall apply as a one-time cost.

Please see ANNEX 1 for the detailed service initiation rate as of 12 February 2024.

Please note that service initiation rate fluctuates as NATO price is determined by a discounted price based on vendor global list prices. If the list price changes, the NATO price consequently changes as well.

Service delivery time for new requests are 3 business days subject to local availability of items on stock.

Annex 1

Service Type	COTS	TEMPEST-C	TEMPEST-B	TEMPEST-A	Service Initiation SSC (EUR)		Remarks
NDW003-A Static Desktop (Workstation) Device	Not Available	1,770	1,902	3,887	186.41		Fixed HDD
NDW003-A Static Desktop (Workstation) Device	Not Available	3,291	3,422	5,408	186.41		Removable HDD

Service Type	COTS	TEMPEST-C	TEMPEST-B	TEMPEST-A	Service Initiation SSC (EUR)		Remarks
NDW003-C Portable (Laptop) Device	1,586	Not Available	Not Available	Not Available	186.41		Docking station and protective case accessories to be procured separately

NDW004 Hybrid Work Environment – Audio-Visual Services

Service ID: NDW004

Service Name: Hybrid Work Environment – Audio Visual Service

Portfolio Group: NATO Digital Workplace Services

Service Status: Pipeline

Service Description: The Hybrid Work Environment, Audio-Visual Service provides collaborative meeting space solutions, comprehensive collaboration and digital learning solutions advice, guidance, design and consultancy support within Audio-Visual expertise across the NATO Enterprise and its external partners. The service includes both consultancy about existing AV setup and new requirements.

The Service offers an extensive selection of audio-visual solutions such as; Audio-Visual Solution and product advice, Design and engineering of (complex) audio and video systems, Installation of audio and video systems, maintenance and repair of audio and video systems as well as proactive monitoring.

Our team of experienced audio-visual engineers is dedicated to provide high-quality audio-visual systems, with an emphasis on reliability, sustainability and long-term customer satisfaction.

We strive to ensure, that our customers receive the best possible audio-visual solutions, customized to their requirements and needs. Through the expertise, quality assurance process and proper training our AV Engineers guarantee that our customers can make the most of their audio and video systems.

The Hybrid Work Environment, Audio-Visual Service excludes automatic procurement of new devices when they have reached their life expectancy. Similarly, the service excludes the cost life-cycle replacement of obsolete equipment.

Value Proposition: The Service ensures that Audio-Visual Solutions are tailored to the unique needs of each customer while being in line with NATO Enterprise policies and guidance on Communications and Information Security. Our team of experienced audio-visual engineers can provide comprehensive design consultancy services, from creating detailed design briefs and technical requirements, to identifying and analysing suitable equipment, to preparing design drawings and schematics. We will provide installation support services through site-surveys and coordinate with Industry Partners to ensure a smooth installation process.

The Hybrid Work Environment – Audio-Visual Service ensures active obsolescence management can be provided, i.e. that the customers have an always accurate overview of their devices (assets) and their associated life-expectancy enabling entities to proactively plan and budget for life-cycle replacement.

Service Flavours: The Hybrid Work dEnvironment - Audio-Visual service types:

NDW004-A Collaboration-Space Solutions – Collaboration-Space Solutions tailored to specific customer requirements. All flavours will receive the below service support as standard.

Service support:

- Site surveys
- Delivery and Installation
- Site acceptance
- Documentation
- User training

Space Flavour:	Standard Features:	Optional:
Personal Conferencing	✓ VTC Integration ✓ 24 inch Touchscreen	✓ 55inch monitor ✓ Poly TC10 Touch panel ✓ Wall mounted or with stand
Small Collaboration spaces	✓ VTC Integration (BYOM) ✓ Up to 55 inch single monitor ✓ 10 inch Touch Panel ✓ Wall mounted or with stand ✓ Standard Monitoring	✓ VTC Integration (CODEC version) ✓ Daily room Monitoring ✓ 360 degree Camera
Standard Collaboration Spaces	✓ VTC Integration ✓ Up to 75 inch dual monitors ✓ 10 inch Touch Panel ✓ Wall mounted or with stand ✓ Standard Monitoring	✓ Centralised Room Control ✓ Executive Monitoring ✓ 360 degree Camera
Executive Collaboration Spaces	✓ Solution design ✓ VTC Integration ✓ Up to 86 inch dual monitors ✓ 10 inch Touch Panel ✓ Executive level enclosure ✓ Room Control ✓ Executive Monitoring	✓ 360 degree Camera ✓ Bespoke furniture

Conference Centres, Auditoria, Control Rooms	✓ Solution design ✓ IP Video Distribution ✓ LCD Video Wall ✓ PTZ Camera's + Automated tracking ✓ Ceiling Microphones ✓ Sound Solution ✓ Executive Monitoring	✓ LED Video Wall ✓ Discussion System ✓ VTC Integration
Custom Solutions	✓ On Demand	

NDW004-B Digital Signage Service - Standardized networked Enterprise-wide hardware (large format display and signage receiver) and software platform solution with user customizable screen zones (option of adding tailored content). Space Reservation is a feature under Digital Signage Service that planned for future released. It will be available through room touch panels/interactive large formats displays/mobile application and web application.

NDW004-C IPTV Service - Standardized networked Enterprise-wide hardware (large format display and IPTV receiver) and software platform solution. The feature offers streaming of TV Channels, Digital Events (e.g. Town Halls, All Hands) to end devices such as IPTV Set-Top Boxes, Large Format Displays or WPS001 devices.

NDW004-D Video Walls – Large video walls including Integrated Control Room Solutions for Operation Centres.

These solutions offer:	Service support:
▪ Scalable Video Walls ▪ Video Distribution ▪ VTC Integration ▪ IPTV Integration ▪ Automated Camera Control ▪ Discussion System Integration ▪ Lecterns	▪ Site surveys ▪ Project implementation ▪ Site acceptance ▪ Documentation ▪ User training

NDW004-E Digital Learning Services - NATO Digital Learning Solutions (DLS) provide information and technology-related learning platforms, to NATO Education and Training facilities (NETF).

These solutions offer:	Service support:

▪ Hybrid and Virtual (VILT[1]) Classrooms ▪ Classroom automation ▪ Learning Management Systems (LMS) ▪ Advanced Distance Learning Solutions (ADL)	▪ Site surveys ▪ Project implementation ▪ Site acceptance ▪ Documentation ▪ User training

Hybrid Work Environment Audio-Visual Service flavours are available on:

Service Type	NATO Unclassified	NATO Restricted	NATO Secret[2]	Mission Secret
NDW004-A	✓	✓	✓	✓
NDW004-B	✓	✓	X	X
NDW004-C	✓	✓	X	X
NDW004-D	✓	✓	✓	✓
NDW004-E	✓	✓	X	X

Please note: For devices used on the high side (NS/MS), TEMPEST testing of each devices is mandatory. The cost for TEMPEST testing is a one-time only cost, which will be included in the Service Initiation cost. The Annual Service rate for both TEMPEST and non-TEMPEST tested devices remains the same.

Service lifecycle for devices: The below table shows life expectancy per device category, the service owner shall inform the entity utilising the device before life expectancy reaches within a suitable time frame.

Service Component	Life Expectancy
NDW004-A Collaboration-Space Solutions	5 Years
NDW004-B Digital Signage Devices	5 years
NDW004-C IPTV Service Devices (set-top Box)	3 Years
NDW004-D Video Walls	8 Years
NDW004-E Digital Learning Services	5 Years

[1] Virtual Instructor-Led Training Facility

[2] TEMPEST testing of devices used on High Side (NS/MS) is mandatory

Service Cost/Price:

The unit of measure, used for service costing is:

Service Component	Unit of Measure	Service Component	Unit of Measure
NDW004-A	Per Solution	**NDW004-D**	Per Solution
NDW004-B	Per Device	**NDW004-E**	Per Solution
NDW004-C	Per Device		

Service ID	Service Name	Service Type	Service Unit	Service Rate 2025 (EUR)
NDW004	Hybrid Work Environment Audio-Visual Service	NDW004-A[1] Collaboration-Space Solutions	Personal Conferencing	1000
			Small Collaboration spaces	2500
			Standard Collaboration Spaces	5000
			Executive Collaboration Spaces	10000
			Conference Centres, Auditoria, Control Rooms Custom Solutions	15 % of total investment cost
		NDW004-B Digital Signage Services	Per Location Per Device	5000 600
		NDW004-C IPTV Services	Per location Per Device	5000 960
		NDW004-D Video Walls	Displays 2X2 Displays 3x3	4200 10125

[1] Service cost for audio-visual components only.

		NDW004-E Digital Learning Services	One Room™ Solution	24000
			Hybrid Solutions Per room	7500
			Classroom Automation Per room	1000

Standard Service Support Levels:

General Service availability target is 99.0% with Priority Resolution Times and Generic Service Priority Assignment Matrix in accordance with the NCI Agency standardised Service Level Agreements in force.

- Standard Support: 08:30 - 17:00 (included in standard service rate)
- VIP Support: 06:00 - 22:00 (service rate available upon request)
- VVIP Support: 00:00 - 23:59 (i.e. 24/7 support) (service rate available upon request)

Proactive Monitoring of Audio Visual systems:

- Standard Monitoring: Weekly checks
- Executive Monitoring: Daily checks

Service initiation cost:

For customers who are procuring new quantities of the service, the service initiation rate (procurement and deployment of the service components) shall apply as a one-time cost.

Please see ANNEX 1 for the detailed service initiation rate as of 12 February 2024.

Please note that service initiation rate fluctuates as NATO price is determined by a discounted price based on vendor global list prices. If the list price changes, the NATO price consequently changes as well.

Service delivery time for new requests are subject to local availability of items on stock or depending on delivery time after order placement.

Annex 1: Hardware and service initiation rates.

Service Type	COTS (EUR)	TEMPEST-C (EUR)	TEMPEST-B (EUR)	Service Initiation (EUR)	Remarks
Personal Conferencing	6000	8000	9000	1500	

Small Collaboration Space	7500	9500	10500	1875	
Standard Collaboration Space	12500	15500	16500	3125	
Executive Collaboration Space	30000	35000	37500	7500	
Custom Solutions	TBD	TBD + 25%	TBD + 30%	25% of COTS	

Service Type	COTS (EUR)	TEMPEST-C (EUR)	TEMPEST-B (EUR)	Service Initiation (EUR)	Remarks
NDW004-B Digital Signage Solutions SDM	750	N/A	N/A	300	
NDW004-C IPTV Solutions Hardware	300	N/A	N/A	300	
NDW004-D Video wall configuration 2by2	30000	37500	3900	7500	Total 4 screens
NDW004-D Video wall configuration 3by3	67500	84375	87750	16875	Total 9 screens
NDW004-E Digital Learning Solutions	160000	N/A	N/A	64000	Pricing related to a 6 Screen configuration one Room™ setup.

NDW005 Digital Events Service

Service ID: NDW005

Service Name: Digital Events Service

Portfolio Group: NATO Digital Workplace Services

Service Status: Available

Service Description: This Service enables the successful delivery of Digital and Hybrid Events to NATO Staff. The range of supported event types includes Digital and Hybrid Events such as town halls, global meetings, summits, conferences, symposiums, committee meetings, webinars. The service provides an inclusive and rich end-to-end digital experience including event planning, event orchestration and management, technical support and offers a tailored event engagement platform.

Value Proposition: The service, delivered by Digital Events (DE) supports NATO staff to achieve their objectives by providing collaboration services, from basic but still formal meetings to complex global digital events. Events are enhanced with a variety of audience engagement tools, event registration options, technologically advanced studio equipment ensuring an integrated and interactive experience for stakeholders and participants and a comprehensive data report post event. The event can be purely digital or hybrid where a traditional physical event is expanded with a virtual component to reach a wider audience, include participants from several remote locations. In addition, engagement features and information retention options extend the life of the event. The digital experience is designed to meet the event's objectives and tailored towards the customer's requirements. The service allows a customer to focus on content and delivery, achieving a successful outcome of the event while the DE takes responsibility for all or part of the event orchestration ensure a flawless delivery.

Service Types: The Service provides a selection of features (depending on a type) that shape your digital event. The features will be adjusted to the audience, classification and platform used for your event. For an overview of features see service types:

NDW005-A Digital Event - digital connect on one of the available platforms (DE to decide the right platform depending on classification level and requirements). The audience for this event is purely digital. This event concerns a digital connect where multiple people connect online to discuss, inform or engage with each other. It can contain one or multiple speakers and offers opportunity for simple content sharing.

Service support:

- Live streaming (customized technical design)
- Personalized and pre-scheduled Event link
- Q&A, Polling, Chat
- Personalized registration for attendees
- Lobby Management: Identity and Access Controls
- Technical Rehearsal
- Event moderation during live event
- Event Recording (including up to 8 hrs of video editing)

- Post Event Analytics

DE roles included: Event Planner/Event Coordinator

NDW005-B Digital and Hybrid Event - hybrid/digital connect including studio connect (provided by customer). The event will be streamed to an online platform (DE to decide the right platform depending on classification level and requirements). The audience for this event can be digital or hybrid, meaning they either connect online or from a viewing room/studio. DE will stream the feed provided by the customer. To provide this stream the requirement from the customer is that they have their own studio/AV set up available. DE provides the online experience from registration to rehearsal and live event and rehearsals will be held to ensure the right connectivity between the platform and studio. Studio means a location equipped with enough AV equipment to capture a feed and stream it to the platform. The location can be an auditorium, conference room, professional TV studio etc. and can be located in any of the NATO offices. A detailed event data report is provided post event.

Service support:

- Live streaming (customized technical design)
- Personalized and pre-scheduled Event link
- Q&A, Polling, Chat
- Personalized registration for attendees
- Lobby Management: Identity and Access Controls
- Technical Rehearsal with Studio
- Event moderation during live event
- Event Recording (including up to 8 hrs of video editing)
- Post Event Analytics
- Studio integration

DE roles included: Event Planner/Event Coordinator

NDW005-C Digital & Hybrid Event with studio (Customized Digital Event - Price through CRF) - Hybrid/digital event where there is a connection from a studio. The studio can be set up on requested location (depending on classification level and requirements), equipment will be provided by DE. The event will be streamed to an online platform (DE to decide the right platform depending on classification level & requirements). A variety of options can be added to achieve the right level of event support. A selection of service support available:

Service Support Basic:

- Live streaming (customized technical design)
- Personalized and pre-scheduled Event link
- Q&A, Polling, Chat
- Personalized registration for attendees
- Event Instructions, welcome slides and virtual backgrounds
- Lobby Management: Identity and Access Controls
- Technical Rehearsal with Studio
- Event moderation during live event
- Event Recording
- TV Studio set up (including mobile equipment: camera/mics/streaming equipment etc.)
- Stage coordination

- Detailed Event Analytics & Lesson Learned (KPIs)
- Speaker Management and rehearsal

Service Support Optional:

- Script writing based on the Agenda
- Technical setup for simultaneous interpretation
- AV set up for complex studio solutions
- Virtual Networking Opportunities
- Hybrid Breakout Sessions
- Content Creation (Video/Presentation design)
- Mobile Devices Integration - digital event experience extended to support mobile devices
- Sourcing and preparing Event host
- Content Manager
- Copywriter for presentations and communication material
- Customer Success

DE roles included: Event Planner/Event Manager/Event Coordinator/Production Manager

Service Ordering and Request:

The event can be purchased either through CRF or as part of the SLA. If Digital Events services are purchased under the SLA, access will be granted to the event-booking tool DEMT. Through this tool the events can be booked. Once the event request is received, DE will schedule an intake meeting after which can be proceeded with exact requirements. An overview of steps below:

1) Intake meeting: to understand the scope and requirements of the event (**Customer & DE**)
2) Platform set up: streaming platform will be customized as per requirements (**DE**)
3) Technical Rehearsal: (**Customer & DE**)
4) Event Delivery: (**Customer & DE**)
5) Post Event Delivery: (**Customer & DE**)

Service Cost/Price:

As every event is unique in terms of audience and outcome, the Digital Events Service is priced “per size of event”. In addition to the 2 event types mentioned under this service, there is the option to request a personalized, NDW005-C, event outside of the defined events. The final cost depends on the complexity of the event and the number of roles requested to be performed by the NCI Agency. The roles (B5/A2 equivalent) will be calculated in accordance with the valid NCI Agency Customer Rates.

NATO Communications and Information Agency

Costed Customer Services Catalogue