Reference Document	Reference ID *(BI, SOW requirement, SRS requirement)*	Desription	Bid Reference	Remarks	Compliance statement
BI	[BI – 3.2.2]	Part 2 is the Technical Proposal provided as a1 .zip File Submitted by Email not larger than 20MB total, which includes: • Volume 1, Engineering, text document: 1 PDF file • Volume 2, Supportability, text document: 1 PDF file • Volume 3, Management text document: 1 PDF file • Annex, Bid Requirements Cross Reference Matrix (BRCM) (BRCM): 1 Excel file If necessary, the technical volume may be separated into more than one email. Maximum email size per each email is 20MB total			
BI	[BI – 3.4.1]	The Bidders Technical Proposal is organised and submitted in three volumes: 3.4.1.1 Volume 1 – Technical – covering requirements from Sections 1, 5, 7, 8, 10, 11 and Annex A, C and H of the SOW; and 3.4.1.2 Volume 2 – Supportability – covering requirements from Sections 6, 7, 11, 12, 13, 14, 15 and Annex A, C and F of the SOW. 3.4.1.3 Volume 3 – Management – covering requirements from Sections 1, 2, 3, 4, 5, 6, 7, 9, 10, 14, 15 and Annex A and B of the SOW, and an Executive Summary of the entire Technical Proposal;			
BI	[BI – 3.4.2]	The mapping of SOW sections to volumes has been done to facilitate a consistent organisation of the Technical Proposal and its subsequent evaluation. Bidders adhere to the mapping, even if individual requirements within sections of the SOW may seem to more logically belong in a different volume. Requirements that are answered in Volumes other than as indicated in paragraph 3.4.1 will not be evaluated			
	[BI – 3.4.3]	The proposed Technical Solution is not “conditional” in nature.			
BI	[BI – 3.4.6.3.1	The Bidder provided an initial System Design Specification (SDS) which describes its proposed technical solution and demonstrates its understanding of the requirements and security requirements as stated in in the SRS			
BI	[BI – 3.4.6.3.2]	The initial SDS follows the outline of SOW Section 15			
BI	[BI – 3.4.6.3.3]	The initial SDS includes an initial Product Breakdown Structure (PBS).			
BI	[BI – 3.4.6.3.4]	The initial SDS demonstrates a comprehensive understanding of all of the requirements of SRS(SOW Annex A) and describe how every requirement is addressed in the Bidder’s proposed solution.			
BI	[BI – 3.4.6.3.5]	In particular, the initial SDS describes how the following requirements are planned to be addressed: (a) System Architecture (b) The following Operational and Systems Views, as defined in the NATO Architecture Framework (NAF, [NAC AC/322-D(2007)0048, 2007]): (c) NOV-1, High-Level Operational Concept Diagram; (d) NSV-1 Systems Interface Description (Composition); (e) NSV-1 System Interface Description (Intra System); (f) NSV-1 System Interface Description (Inter System); (g) NSV-2, Systems Communications Description; (h) NSV-2a: System Port Specification; (i) NSV-4 System Functionality;			

BI	[BI – 3.4.6.3.6]	The initial SDS addresses Interface Dependencies and Constraints. In particular all separate interfaces described in SOW Annex A must be described in the Bidder's design.			
BI	[BI – 3.4.6.3.7]	The initial SDS contains rationale which convinces that performance requirements defined in Book II, Part IV SOW, Annex A will be met.			
BI	[BI – 3.4.6.3.8]	The initial SDS shows clear traceability between the Contractor's design and the requirements in Book II, Part IV SOW Annex A.			
BI	[BI – 3.4.6.4.1]	For bidding purposes only, in volume 2, the Bidder commits to meet all requirements described in SOW Section 7 for overall system engineering			
	[BI – 3.4.6.5.1]	The Bidder provided an initial System Implementation Plan (SIP), which describes its proposed approach to meeting of the requirements of SOW Section 7			
BI	[BI – 3.4.6.5.2]	The initial SIP follows the outline from Book II, Part IV SOW Section 15			
BI	[BI – 3.4.6.5.3]	The initial SIP covers the entire implementation scope (Book II, Part IV SOW, Annex C)			
BI	[BI – 3.4.6.5.4]	The initial SIP demonstrates a clear understanding of the services to be implemented and describe the Bidder's approach to migration of users.			
BI	[BI – 3.4.6.5.5]	The initial Migration Plan included in the initial SIP fully describes the Bidder's methodology and approach to the migration, including the stages he proposes be followed, the testing to be done, the roll back capabilities proposed and the way in which risks will be managed during the migration process.			
BI	[BI – 3.4.6.5.6]	For bidding purposes only, the Bidder assumes that all elements of its design must be provided in full at the implementation stage and that no hardware , software or business processes exist on site in a reusable form.			
BI	[BI – 3.4.6.5.7]	The initial SIP describes the Bidder's approach to site surveys, identify the issues to be checked on site and relate the site survey to the overall implementation effort in terms of timing and purpose, in accordance with SOW sections 7, 9, and 15.			
BI	[BI – 3.4.6.5.8]	The initial SIP identifies all information to be collected during site surveys, including locations and facilities which need to be inspected.			
BI	[BI – 3.4.6.5.9]	The initial SIP describe the size of team and level of effort involved for site surveys.			
BI	[BI – 3.4.6.5.10]	The initial SIP describe its proposed arrangements to ensure timely and complete delivery and installation of all relevant supplies and equipment			
BI	[BI – 3.4.6.5.11]	The initial SIP describe its proposal for the implementation of the IEG-C Reference System			
BI	[BI – 3.4.6.5.12]	In all descriptions provided, the Bidder is clear regarding how its approach minimises disruption to existing services.			
BI	[BI – 3.4.6.6.1]	The Bidder provided an initial Master Test Plan (MTP), which describes its proposed approach to meeting the requirements of SOW Section 8			
	[BI – 3.4.6.6.2]	The initial MTP describes a coherent high level approach to testing, verification & validation, providing initial scope and schedule on the TVV phases as required in SOW Section 8, Table 14.			
	[BI – 3.4.6.6.3]	The MTP is consistent with other bid documents such as the PMS and the SIP: MTP activities be included in the PMS and products be described in the PBS.			
	[BI – 3.4.6.6.4]	The Bidder provided an initial Defect Reporting and Management Plan, which describes its proposed approach to meeting the requirements of SOW Section 8.			
	[BI – 3.4.6.6.5]	The bidder provided 2 exemplary test cases on how to meet two specific requirements SRS-4-141 and SRS-6-70. Test cases be compliant with the SOW clauses and templates provided			

	[BI – 3.4.6.7.1]	The Bidder described their input to the security accreditation documentation in support of the accreditation process as part of the initial PIP in accordance with Section 10 of the SoW: (a) CIS Description (b) Security Risk Assessment (SRA) Report (c) Generic System Interconnection Security Requirements Statement (SISRS) (d) Security Operating Procedures (SecOPs) (e) Security Test and Validation Plan (STVP)			
	[BI – 3.4.6.7.2]	The Bidder provided a CIS Description document to include at a minimum but not limited to, the following information: (a) Detailed technical description showing the main components and the high level as well as detailed information flows, (b) Description of all internal and external connections of the system, (c) List of hardware and software components used,			
	[BI – 3.4.6.7.3]	The Bidder provided an initial qualitative Security Risk Assessment (SRA), which describes its proposed technical solution and demonstrates its understanding of the requirements in Section 10 of the SOW.			
	[BI – 3.4.6.7.4]	The initial SRA is developed in accordance with "Guidelines for Security Risk Management (SRM) of Communication and Information Systems (CIS) (Ref. AC/35-D/1017-REV3)" and include the following: (a) Identification of the scope and objective of the security risk assessment; (b) Determination of the physical, personnel and information assets which contribute to the fulfilment of the IEG-C; (c) Determination of the value of the assets (very low – low – medium – high – very high); (d) Identification of the threats and vulnerabilities to the risk environment and their level; (e) Identification of existing security measures (e.g. assertions about physical and personal security measures already in place at NATO sites); (f) Identification of countermeasures proposed in the Bid; (g) Determination of of risk value after implementation of security measures listed in points (e) and (f)			
	[BI – 3.4.6.7.5]	The Bidder provided an initial Generic System Interconnection Security Requirements Statement (SISRS) that: (a) Describe the security measures mandated by NATO Security Policy and supporting directives (b) Describe the minimum levels of security deemed necessary to countermeasure the risk(s) identified in a risk assessment; (c) have a unique identifier for each security requirement; (d) Indicate mandatory and recommended Security Mechanisms (SMs). (e) System Interconnection Security Requirement Statement (SISRS) template under Annex F-2 shall be used. For bidding purposes, this template and initial bid submission will be NATO Unclassified.			
	[BI – 3.4.6.7.6]	The Bidder provided initial Security Operating Procedures (SecOPs) to include as a minimum the following procedures: (a) Centralized administration and monitoring of IEG-C; (b) Backup & recovery; (c) Emergency procedures; (d) Security Test and Verfication Plan (STVP) template under Annex F 1 shall be used. For bidding purposes, this template and initial bid submission will be NATO Unclassified.			
	[BI – 3.4.6.7.7]	Initial Sec OPs also cover all security requirements identified in the SRA and SSRS which are not fully fulfilled by technical countermeasures			
	[BI – 3.4.6.7.8]	The Bidder provided an initial STVP that describes the security testing and verification of the CIS Security measures to be implemented. A complete and detailed sequence of steps to be followed proving that the security mechanisms designed into IEG-C enforce the security requirements identified in the SISRS. The STVP contain traceability matrix between tests and SISRS requirements			

	[BI – 3.4.6.7.9]	For each STVP security test the following details are identified: (a) The objective of the security test; (b) An outline description of the security test; (c) A description of the execution of the security test (too include technical instructions how to conduct the test); (d) The pass criteria for the security test. (e) Reference to applicable SISRS requirement(s); (f) Reference to applicable Security Mechanism(s).			
	[BI – 3.4.6.7.10]	~~The Bidder described the STVR for every instance of security testing conducted based on the STVP~~			
BI	[BI – 3.4.6.7.11]	~~For each STVR security test the following details are identified:~~ ~~(a) Test ID;~~ ~~(b) An outline description of the security test;~~ ~~(c) Detailed results of the security tests;~~ ~~(d) Test status (e.g. in progress, passed, failed)~~ ~~(e) Test completion (in per cent);~~ ~~(f) Failure severity (e.g. critical, serious, major, less important, none);~~ ~~(g) Test date;~~ ~~(h) Information about who conducted the test;~~ ~~(i) Information about who witness the test~~			
	[BI – 3.4.6.7.12]	~~STVR contain overall test summary details:~~ ~~(a) Identification of the element under tests;~~ ~~(b) Tests starting date;~~ ~~(c) Tests finishing date;~~ ~~(d) Amount of all tests to be conducted;~~ ~~(e) Amount of tests executed;~~ ~~(f) Tests passed;~~ ~~(g) Tests failed;~~ ~~(h) Tests still in progress~~			
	[BI – 3.4.6.7.13]	The bidders provide a supply chain security statement for security enforcing products, according to AC/322-D(2017)0016.			
	[BI – 3.4.6.7.14]	The bidders provided a statement confirming that only evaluated boundary protection devices (e.g. guards) have been proposed. The evaluation be according to Common Criteria or National equivalent, in accordance with AC/322-D/0030-REV5.			
BI	[BI – 3.4.6.7.15]	The bidders provided a statement confirming that only Tempest tested hardware (compliant with SDIP-29/2) have been proposed. Alternatively bidders can consider and propose usage of Tempest racks (compliant with SDIP-29/2).			
	[BI – 3.4.7.2.1	Integrated Logistics Support The Bidder provided a draft Integrated Logistics Support Plan in accordance with the SOW requirements including the required sub-sections and content with sufficient details to demonstrate the Bidder's ability to perform the ILS activities.			
	[BI – 3.4.7.2.2	The Bidder demonstrate its understanding and compliance with all the SOW requirements by creating appropriate subsections and detailing the requirements with actual proposed activities.			
	[BI – 3.4.7.2.3	The Bidder provided a detailed approach for the Design Influence (RAMT and LSA) areas for the actual analyses, documenting the analysis, tools, skills and relation with SRS and design in general.			
	[BI – 3.4.7.2.4	The Bidder detailed the different Maintenance and Support Levels, the interfaces between these different levels, maintenance and support environment, constraints, locations, procedures, artefacts, organisation, personnel skills, related ITIL processes and responsibilities between different parties to maintain the delivered baselines of the system in different phases of the lifecycle.			

	[BI – 3.4.7.2.5	The Bidder detailed its approach for the Initial Operational Support and warranty requirements, details the activities based on each party's responsibilities including the proposed services, response times, organization and planning in accordance with the SOW requirements.			
	[BI – 3.4.7.2.6	The Bidder detailed its approach for the Supply Support and PHST requirements and details the proposed activities in accordance with the SOW requirements.			
	[BI – 3.4.7.2.7	The Bidder demonstrated that all ILS activities and milestones are integrated into the project master schedule.			
	[BI – 3.4.7.3.1]	Draft Support Case The Bidder provided a draft Support Case, as detailed in the SOW section 6.4. The Support Case provide sufficient details to show the Bidder's approach and capability to perform the required LSA and RAMT studies, including how the proposed design take the SOW and SRS RAMT requirements into consideration.			
	[BI – 3.4.7.3.2]	The Bidder demonstrated its understanding and compliance with the Support Case requirements by creating appropriate subsections and detailing the requirements with actual proposed activities to show the Bidder's approach and capability to perform the required LSA and RAMT studies, including how the proposed design take the SOW and SRS RAMT requirements into consideration.			
	[BI – 3.4.7.4.1]	Configuration Management The Bidder provided a draft Configuration Management Plan (CMP) which describe how Configuration Management be performed in accordance with the requirements of the SOW Section 12			
	[BI – 3.4.7.4.2]	The Bidder provided details to demonstrate its understanding of the CM process on how it be planned, managed, resourced, executed and provided including the organization and personnel, CM tools, directives and standards, meetings, reviews and deliverables (baselines, documents, CMDB etc.).			
	[BI – 3.4.7.4.3]	The Bidder provided the Configuration Management Plan in the structure and detailed content in accordance with the SOW requirements including minimum the 'Organization, Configuration identification and Documentation, Baselines, Configuration control, Interface management, Change request Process, Configuration Status Accounting, Configuration Audits and Reviews and Configuration Management Tools'.			
	[BI – 3.4.7.5.1]	Quality Assurance The Bidder provided a draft Quality Assurance Plan (QAP) which conforms to the requirements detailed in Section 11 of the SOW.			
	[BI – 3.4.7.5.2]	The Bidder demonstrated that the Quality Management System is in place for the project in accordance with AQAP-2110 and /or equivalent ISO standards.			
	[BI – 3.4.7.5.3]	The Bidder demonstrated its understanding of the QA requirements of this project by detailing the QA procedures for requirements analysis, design, development, production, installation, test, acceptance, certification, support, defects and corrective actions, documentation, reviews and audits including subcontractor management specified for this project.			
	[BI – 3.4.7.6.1]	Training The Bidder provided a draft Training Plan describing how he conduct the Training Needs Analysis (TNA), and provide the necessary training courses in accordance with Section 6 of the SOW.			
	[BI – 3.4.7.6.2]	The Bidder demonstrated its understanding and compliance with Training Program requirements by explaining how the Bidder will schedule, resource and manage the various training requirements (TNA, training schedule, training courses and material, training tools, media, training personnel, training reviews, meetings, assessment, evaluation and reporting) starting from the contract award until the acceptance.			
	[BI – 3.4.7.6.3]	The Bidder demonstrated its understanding of the Training Needs Analysis (TNA) concept based on the references from Bi-Sc and experiences from other projects by explaining how the Training Needs Analysis will be performed with all possible deliverables, inputs and outputs to the process.			
BI	[BI – 3.4.8.3.1]	Bidders provided an overview of the salient features of their technical Bid in the form of an executive summary.			

BI	[BI – 3.4.8.3.2]	The Executive Summary provided a general description of the major points contained in each of the required sections of the technical proposal (i.e., 3 volumes) and demonstrate the depth of the Bidder's understanding of: the project, the implementation environment, the problems and risks of project implementation foreseen by the Bidder, and the Bidder's ability to communicate high level concepts in an appropriate and succinct manner. The Bidder highlight the strengths which it and its team bring to the project in terms of minimising the problems and reducing the risks, while meeting the overall schedule, and the key points of the technical approach. This summary not exceed 10 pages.			
BI	[BI – 3.4.8.3.3]	Bidders explicitly stated in the Executive Summary that, should their firm be selected and awarded the contract resulting from this solicitation, the delivered product(s) and services comply with the requirements of the Statement of Work (including all annexes).			
BI	[BI – 3.4.8.4]	Bidders compiled a detailed Table of Contents which lists not only the section headings but also the major sub-sections, and topic headings of the Bid.			
BI	[BI – 3.4.8.5.1]	The Bid demonstrated the Bidder's understanding of the Purchaser's requirements as described in the Statement of Work (SOW), Book II Part IV. The strategic vision behind the IE-C project, the objectives, constraints and scope must all be addressed and related to the technical solution described in the Bid.			
BI	[BI – 3.4.8.6.1]	Bidder Qualifications and Key Personnel Volume 3 describe the company structure and activities of the prime Contractor. The country in which the prime Contractor is registered be identified and the size and location(s) of the company headquarters and subsidiary branches described. Within that structure the location and organizational unit of the office which will manage this Contract be identified. This section also describe the major activities of the company and how they are distributed across the organisation.			
BI	[BI – 3.4.8.6.2]	The Bid provide a description of the corporate capabilities of the Bidder, including corporate experience, corporate structure and individual skills and experience. In particular, the Bidder provide evidence of relevant and recent experience in the design, integration, testing, and implementation of projects similar to the IEG-C Project. The Bidder provide a section which describes how the experience and expertise of the prime Contractor and all nominated sub-Contractors will contribute to the successful execution of the Contract.			
BI	[BI – 3.4.8.6.3]	The Bidder provide a section which identifies its major proposed sub-Contractors for the Project. Major proposed sub-Contractors, for purposes of this section, refer to the criteria set forth in Clause 10 of the Prospective Contract General Provisions entitled "Sub-Contracts". The Bidder identify the firm and the nation of origin and describe the contribution which the sub - Contractor is expected to make to the execution of the project. The Bidder also provide rationale for the selection of the sub-Contractor and describe the added value the sub-Contractor will bring to the execution of the project.			
BI	[BI – 3.4.8.6.4]	Volume 3 provide a description of individual skills and experience in relation to the project of all project team members and Subject Matter Experts (SMEs) foreseen to support the project team. The description include how each individual expertise and experience will add value to the team.			
BI	[BI – 3.4.8.6.5]	Volume 3 provide the resumes / Curricula Vitae (CV) and supporting certification documentation (e.g. Prince 2 certificates) of each proposed Key Personnel that meet or exceed the requirements in SOW Section 13.			
BI	[BI – 3.4.8.6]	Project Management In order to demonstrate how the Bidder plans to approach the management of the project (according to Section 4 of the SoW), the Bidder submit initial versions of the Project Implementation Plan (PIP) to include the Project Management Plan (PMP), of the Work Breakdown Structure (WBS), of the Product Breakdown Structure (PBS) and Product Flow Diagram (PFD); Project Master Schedule (PMS); and identify all acitivites related to the security accreditation process (according to Section Section 10 of the SoW).			
BI	[BI – 3.4.8.6]	The Bidder submitted a preliminary Project Implementation Plan (PIP) in accordance with the requirements of Section 4 and 15 of the SOW, which clearly describes how the Bidder intends to implement the totality of the project in compliance with the contractual requirements and the following specific requirements:			

BI	[BI – 3.4.8.7.2.1]	Project Overview. The Bidder provided the Project Overview which provide an executive summary overview of the offered capability. The Project Overview also summarise the main features of each of the sections of the Technical Proposal and indicate in broad detail how the Project will be executed during the full lifetime of the Project;			
BI	[BI – 3.4.8.7.2.2]	The PIP includes a preliminary Project Management Plan (PMP) that defines how the Bidder intends to manage this project from contract signature through Final System Acceptance and throughout any warranty periods. The PMP consider all aspects of project management and control and demonstrate how all the critical dates defined in the contract will be met;			
BI	[BI – 3.4.8.7.2.3]	The PIP includes a Project Master Schedule (PMS) that contain all contract events and milestones for the Project. The PMS show all contractual deliverables, their delivery dates, and the tasks associated with them. The PMS for each task identify the start and finish dates, duration, predecessors, constraints, and resources. The PMS provide network, milestone, and Gantt views, and identify the critical path for the overall project.			
BI	[BI – 3.4.8.7.2.4]	The Bidder provided a statement assuring that all requirements be met for the Site Survey in accordance to the requirements stated in Section 9 of the SoW, Book II Part IV.			
BI	[BI – 3.4.8.7.2.5]	The submitted documents include sufficient information to demonstrate the Bidder's understanding of the key challenges involved in the IEG-C project, and demonstrate that the Bidder is proposing an approach that can deal with these challenges.			
BI	[BI – 3.4.8.8.1]	The Bidder provided an initial PMP following the structure called for in SOW Section 15, Book II Part IV.			
BI	[BI – 3.4.8.8.2]	The initial PMP demonstrate how the Project Controls required under SOW Section 4 will be implemented during the project. In particular the Bidder demonstrate that the Project Management methodology proposed for the project is suitable to the successful execution of the project.			
BI	[BI – 3.4.8.8.3]	The initial PMP demonstrates the project implementation including its management structure and project management processes, personnel assignments, external relationships necessary to provide the capability as required by this Contract.			
BI	[BI – 3.4.8.8.4]	The initial PMP is sufficiently detailed to ensure that the Purchaser is able to assess the Contractor plans with insight into the Contractor's plans, capabilities, and ability to satisfactorily implement the entire project in conformance with the requirements as specified in the SOW.			
BI	[BI – 3.4.8.8.5]	The initial PMP demonstrated that the Bidder has understood the process imposed in SOW Section 15.9 and describe supporting the cycle of design reviews and approvals.			
BI	[BI – 3.4.8.9.1]	The initial PBS identifies all products and distinguish between management products and specialist products in Section 4 and 15 of the SOW.			
BI	[BI – 3.4.8.9.2]	The PBS includes a hierarchical diagram of all the products (management products and specialist products), having at its topmost product the final product of the overall project, i.e., the IEG-C System.Describe each product (management products and specialist products) including its quality requirements. The product descriptions address sufficient detail to permit management assessment of progress with EVM.			
BI	[BI – 3.4.8.10.1]	The Bidder submitted an initial Project Master Schedule (PMS).			
BI	[BI – 3.4.8.10.2]	The PMS is according to Section 4.4.6 of the SoW.			
BI	[BI – 3.4.8.10.3]	The initial PMS demonstrate in particular include how the bidders plan to apply EVM throught the project implementation duration.			
	[BI – 3.4.8.10.4]	The PMS include additional subordinate milestones that the Bidder plans to achieve which make clear the extent of parallel activities and the detailed phasing and dependencies of different activities.			
	[BI – 3.4.8.10.5]	The PMS meet the project deadlines (EDC + x months) as described in SOW Section 3, Book II Part IV.			

	[BI – 3.4.8.11.1]	Risk Management The Bidder described in the intial RMP how he will implement the Risk Management process according to Section 4 of the SoW, with the minimum details: (a) Overall Risk Management approach (b) Key Risk Management processes (c) Key Risk Categories (d) Risk Prioritization Matrix (e) Risk Management roles and responsibilities (f) Risk Log template which at minimum follow the outline recommended in this SOW (see Section 15.2)			
	[BI – 3.4.8.12.2]	The Risk Log is in accordance with SOW Section 10.2, Book II Part IV .			
	[BI – 3.4.8.11.3]	The following risks are addressed in the Bid listing the risks, and indicating for each one the following information (but not limited to): (a) Risk identifier: unique code to allow grouping of all information on this risk; (b) Description: brief description of the risk; (c) Risk category (e.g., management, technical, schedule, and cost risks); (d) Impact: effect on the project if this risk were to occur; (e) Probability: estimate of the likelihood of the risk occurring; (f) Risk rating (High, Medium, Low); (g) Proximity: how close in time is the risk likely to occur; (h) Response strategy: avoidance, mitigation, acceptance, transference (i) Response plan(s): what actions have been taken/will be taken to counter this risk; (j) Owner: who has been appointed to keep an eye on this risk; (k) Author: who submitted the risk; (l) Date identified: when was the risk first identified; (m) Date of last update: when was the status of this risk last checked; (n) Status: e.g., closed, reducing, increasing, no change.			
	[BI – 3.4.8.11.4]	As part of the initial PMP, the Bidder describe how risks will be managed throughout the execution of the contract in response to the requirements of SOW Section 4			
	[BI – 3.4.8.12.1]	Section 1 of the SOW contains an introduction to the IEG-C project as well as some high level requirements. The Bidder provided a simple affirmation that all requirements will be met			
	[BI – 3.4.8.12.2]	Section 2 of the SOW contains the list of applicable documents. he Bidder provided a simple affirmation that all documents from Section 2 be adhered to			
	[BI – 3.4.8.12.3]	Section 15 of the SOW contains outlines of some IEG-C documents to be delivered. The Bidder provided a simple affirmation that all requirements for these documents will be met			
	~~[BI – 3.4.8.12.5]~~	~~Reserved~~			
BI	[BI – 3.4.8.12.6]	The Bid demonstrates a clear understanding of PFE and describe how the Bidder proposes to make use of / integrate with PFE during the execution of the contract			
BI	[BI – 3.4.9.1]	Part II contains a Bid-Requirements Cross reference Matrix (BRCM) in the format indicated at BOOK I - ANNEX D.			

Reference Document	**Reference ID *(BI, SOW requirement, SRS requirement)***	**Description**	**Bid Reference**	**Remarks**	**Compliance statement**
SOW	[SOW-1]	The Contractor SHALL take due account of all the elements of purpose described in this SOW and ensure during the execution of the contract that the purpose described in this SOW is completely addressed in the products and services provided.			
SOW	[SOW-2]	The Contractor SHALL deliver the IEG-C as detailed in the System Requirement Specifications (SRS).			
SOW	[SOW-3]	The Contractor SHALL provide all necessary resources to include services, personnel, materials, components, equipment[1], data[2] and documentation needed to accomplish all the tasks described in the SOW, to meet all the requirements of the SOW (including annexes) and to fulfil all other Contract provisions.			
SOW	[SOW-4]	The documents listed in SECTION 2: Applicable Documents will be revised over time. The Contractor SHALL always use the current version of each document.			
SOW	[SOW-5]	The Contractor SHALL be aware and comply with above mentioned documents throughout the Contract.			
SOW	[SOW-6]	The Contractor SHALL provide project management services.			
SOW	[SOW-7]	The Contractor SHALL provide systems engineering services to cover: o Requirements review; o System design and o System Integration.			
SOW	[SOW-8]	The Contractor SHALL provide test, verification and validation services to prove the system Product Baseline is meeting its requirements.			
SOW	[SOW-9]	The Contractor SHALL fully document the design, operation, and maintenance of IEG-C by providing the required manuals, operational procedures, supporting technical data, computer software and drawings required by the Contract.			
SOW	[SOW-10]	The Contractor SHALL conduct all necessary activities to obtain Security Accreditation at the NATO SECRET (NS) and applicable Mission SECRET (MS) levels for all installed sites/instances.			
SOW	[SOW-11]	The Contractor SHALL provide System Services as described in SECTION 7			
SOW	[SOW-12]	The Contractor SHALL co-ordinate with the Purchaser to ensure that the site preparation activities are completed in accordance with the installation requirements of the delivered system.			
SOW	[SOW-13]	The Contractor SHALL procure and prepare the system components, as agreed in this contract, for delivery to the sites specified in this Contract.			
SOW	[SOW-14]	The Contractor SHALL deliver the required software to the prepared sites, together with those that may be provided by the customer as PFE, and execute installation/deployment, on-site testing, training, and activation.			
SOW	[SOW-15]	The Contractor SHALL provide support to application and service management integration			
SOW	[SOW-16]	The Contractor SHALL provide Integrated Logistics Support (ILS), including training services, as described in SECTION 6 Integrated Logistics Support (ILS).			
SOW	[SOW-17]	The Contractor SHALL provide operation and maintenance support with appropriate service management interfaces both at information (monitoring / reporting) and process (request / incident) level (see Annex F Maintenance and Support Concept (After FSA)).			
SOW	[SOW-18]	The Contractor SHALL comply with all overarching requirements as described in the SOW (Testing process, Site survey process, Quality Assurance, Configuration Management).			
SOW	[SOW-19]	The Contractor SHALL meet or “exceed” the Notional schedule (see 3.2: Notional schedule).			
SOW	[SOW-20]	The Contractor SHALL be aware and comply with the documents listed in SECTION 2 throughout the Contract.			
SOW	[SOW-21]	The Contractor SHALL note that the above milestones have been defined in a chronological order. The start of activities leading to a milestone requires the acceptance of the previous milestone (for example, the start of system implementation activities (SECTION 13) requires the prior acceptance of the DA milestone).			
SOW	[SOW-22]	The Contractor SHALL adhere to the Overall Project Schedule. Contractor SHALL reflect this in all relevant Project Management Documentation (Section 4.4: Project Management Documentation).			
SOW	[SOW-23]	The Effective Date of Contract (EDC) SHALL be established at the time of Contract Award (CAW).			

SOW	[SOW-24]	The Contractor SHALL integrate IEG-C in its Project Master Schedule at minimum by committing to deliver: o System Requirements Review (SRR) o Preliminary Design Review (PDR) o Critical Design Review (CDR) o Factory Acceptance Test (FAT) o Acceptance of IEG-C security accreditation package o System Integration Testing (SIT) + System Acceptance Testing (SAT)+User Acceptance Testing (UAT) o Deployment Authorization (DA) o Preliminary System Acceptance (PSA) o Site Accreditation (security accreditation of interconnection via particular instance of IEG-C) o Site Acceptance Phase (SA) o Operational Test & Evaluation (OT&E) o Final System Acceptance FSA			
SOW	[SOW-25]	The Contractor SHALL meet or “exceed” the milestones mentioned in the above schedule. “Exceed” SHALL be understood as a situation where the Contractor has delivered earlier than the dates (i.e. EDC + ‘x’ months) mentioned in the above schedule, and the Purchaser has accepted the milestone accordingly.			
SOW	[SOW-26]	The Contractor SHALL implement 11 IEG-C on the sites marked as “Mandatory Sites” in Table Annex B 15 – Site Type and Location of Annex B.1			
SOW	[SOW-27]	The Contractor SHALL propose the implementation sequence of the sites in Master Test Plan. The final sequence will be determined in coordination with the Agency.			
SOW	[SOW-28]	On the exercise of a contract option, the Contractor MAY implement up to 7 additional IEG-C on the sites marked as “Optional Sites” in Table Annex B 15 – Site Type and Location of Annex B.1			
SOW	[SOW-29]	The Contractor SHALL execute all project management activities (see SECTION 4: Project Management) due for each milestone, and all associated deliverables will have been approved by the Purchaser to enable successful completion of each milestone.			
SOW	[SOW-30]	The Contractor SHALL organize and conduct the SRR (EDC+2MO) at the Purchaser’s facility to present the updated SRS with its proposed changes for the design and integration of the IEG-C which will then become the Functional Baseline (FBL).			
SOW	[SOW-31]	The Contractor SHALL use as a main source for SRR the ISO/IEC/IEEE29148 (Systems and software engineering — Life cycle processes — Requirements engineering), the IEEE12207 and the IEE15288 (Systems Engineering).			
SOW	[SOW-32]	The Contractor SHALL review the Contractual IEG-C System Requirements Specification (SRS) and all other applicable documents: o liaise with NATO subject matter experts as necessary; o prepare its recommendations in terms of proposed changes to the System Requirements Specification (SRS); o The Contractor may propose changes to the SRS, in order to resolve inconsistencies and/or make improvements; such proposals SHALL be considered by the Purchaser through the CCB process after Systems Requirements Review Meetings.			
SOW	[SOW-33]	The Contractor SHALL identify any inconsistencies within the requirements or that are in conflict (e.g. with design constraints).			
SOW	[SOW-34]	The Contractor SHALL justify any proposed changes to the requirements by the expected system cost, schedule, performance, and supportability impacts.			
SOW	[SOW-35]	The Contractor's SRS SHALL be the Purchaser provided SRS with approved changes and, as required, extended with additional details supporting the approved scope.			
SOW	[SOW-36]	The Contractor's proposed changes to the SRS SHALL be delivered prior to SRR (EDC+2MO).			
SOW	[SOW-37]	In planning the SRR meeting, the Contractor SHALL include Entry Criteria given in Table 3: The SRR Entry Criteria and make them available to the Purchaser at least two (2) weeks prior to the SRR (EDC+2MO)			
SOW	[SOW-38]	The Contractor SHALL perform a System Requirements Analysis Review (see Section 5.3: System Requirements Analysis and Review).			
SOW	[SOW-39]	The Contractor SHALL update the Change Proposal documentation (see 12.6 Engineering Change Proposals (ECP)).			
SOW	[SOW-40]	During the event the Contractor SHALL collect from the PURCHASER assessment inputs based on Table 4: The SRR Success Criteria and upon conclusion of the SRR the Contractor SHALL produce a report and make it available to the Purchaser at most (1) week after the SRR.			

SOW	[SOW-41]	The Contractor's SRR SHALL be considered completed when the Purchaser and the Contractor have agreed to all necessary changes to the SRS such that the SRS is sufficient to begin or continue with the design and implementation work.			
SOW	[SOW-42]	Review and acceptance of design documentation provided by the Contractor to the Purchaser SHALL not imply Purchaser acceptance of the design. It remains the sole responsibility of the Contractor to prove the design through the regime of testing set forth in the Contract and it SHALL be the sole responsibility of the Contractor in the event that the system proves deficient in meeting the SRS			
SOW	[SOW-43]	The Contractor SHALL perform a System Design as defined in section 5.4.4: Design Reviews, and the associated documentation SHALL have been approved by the Purchaser.			
SOW	[SOW-44]	The Contractor SHALL complete the site survey process as defined in SECTION 9: Site Surveys and deliver the associated reports for approval by the Purchaser for all the sites that form part of PSA scope (Section 3.10: Provisional System Acceptance (PSA)) and SECTION 9: Site Surveys.			
SOW	[SOW-45]	The Contractor SHALL perform the Training Needs Analysis (TNA) for all the sites that form part of PSA scope (Section 3.10: Provisional System Acceptance (PSA)) for approval by Purchaser, as defined in Section 6.6.2: Training Needs Analysis (TNA) - The Contractor SHALL ensure the Training Materials include how the Transition from one Release to the next release is realised and how to install, configure and maintain the Modified or new Component capability, including COTS components.			
SOW	[SOW-46]	The Contractor SHALL deliver the Training Plan that will cover all the sites that form part of PSA scope (Section 3.10: Provisional System Acceptance (PSA)) for approval by Purchaser, as defined in Section 6.6.3: Training Plan.			
SOW	[SOW-47]	The Contractor SHALL have delivered the System Implementation Plan (SIP) for all the sites that form part of PSA scope (Section 3.10: Provisional System Acceptance (PSA) and Section 7.3: System Implementation Plan (SIP)) for approval by Purchaser.			
SOW	[SOW-48]	In planning the PDR (EDC+3MO) meeting, the Contractor SHALL include Entry Criteria given in Table 5: The PDR Entry Criteria and make them available to the Purchaser at least two (2) weeks prior to the PDR			
SOW	[SOW-49]	During the event the Contractor SHALL collect from the PURCHASER assessment inputs based on Table 6: The PDR Success Criteria and upon conclusion of the PDR (EDC+3MO) the Contractor SHALL produce a final report and make it available to the Purchaser at most (1) week after the PDR			
SOW	[SOW-50]	In planning the CDR meeting, the Contractor SHALL include Entry Criteria given in Table 7: The CDR Entry Criteria and make them available to the Purchaser at least two (2) weeks prior to the CDR (EDC+6MO)			
SOW	[SOW-51]	The Contractor SHALL perform a Critical Design Review as defined in 5.4, and the associated documentation SHALL have been approved by the Purchaser.			
SOW	[SOW-52]	The Contractor SHALL complete the site survey process as defined in SECTION 9 and delivered the associated reports for approval by the Purchaser for all the sites that form part of PSA scope.			
SOW	[SOW-53]	The Contractor SHALL update the Training Needs Analysis (TNA) for all the sites that form part of PSA scope (Section 3.10: Provisional System Acceptance (PSA)) for approval by Purchaser, as defined in Section 6.6.2 Training Needs Analysis (TNA) - The Contractor SHALL ensure the Training Materials include how the Transition from one Release to the next release is realised and how to securely install, configure and maintain the Modified or new Component capability, including COTS components.			
SOW	[SOW-54]	The CDR documentation and achievement of the CDR milestone are subject to the Purchaser approval. Unless otherwise approved by the Purchaser, the Contractor SHALL not proceed with the CDR stage without successful completion of the PDR (EDC+3MO) milestone.			
SOW	[SOW-55]	During the event the Contractor SHALL collect from the PURCHASER assessment inputs based on Table 8: The CDR Success Criteria and upon conclusion of the CDR the Contractor SHALL produce a report and make it available to the Purchaser at most (1) week after the CDR.			
SOW	[SOW-56]	The Contractor SHALL have performed necessary activities and satisfied criteria for meeting FAT (EDC+9MO) milestones as defined in SECTION 8 and the associated documentation SHALL have been approved by the Purchaser.			
SOW	[SOW-57]	The milestone “Acceptance of IEG-C security accreditation package” will be achieved when NSAB approval is granted at EDC+13mo.			
SOW	[SOW-58]	The contractor SHALL deliver all documentation according to SECTION 10, 7 months in advance of the expected “Acceptance of IEG-C security accreditation package Milestone” in order to have NSAB approved deliverables before commencing WP 3 / Installation of gateways.			
SOW	[SOW-59]	The Contractor SHALL have performed necessary activities and satisfied criteria for meeting SIT + SAT + UAT (EDC+17mo) milestones as defined in SECTION 8 and the associated documentation SHALL have been approved by the Purchaser.			

SOW	[SOW-60]	The Contractor SHALL comply with the decision of the Purchaser's CAB and only after CAB approval to deploy authorization is granted, the installation of the first site can be initiated based on the Purchaser approved Deployment Plan.			
SOW	[SOW-61]	The Contractor SHALL have handled any change to satisfy the security requirements.			
SOW	[SOW-62]	The Contractor SHALL have delivered the required training (including training for RAs operators) at agreed site(s), according to Training and the training plan approved by Purchaser.			
SOW	[SOW-63]	The Contractor SHALL have completed and have received approval by the SAA of the Security Accreditation Documentation (see SECTION 10), including all the localised versions of documents (see 10.3), for all the (block of) site(s).			
SOW	[SOW-64]	The Contractor SHALL have completed the Site Acceptance Plan and have received the approval by the Purchaser.			
SOW	[SOW-65]	The Contractor SHALL have completed the Site Acceptance Test Cases and have received the approval by the Purchaser.			
SOW	[SOW-66]	The Contractor SHALL have completed the Operational System Acceptance (OSA) Plan and have received the approval by the Purchaser.			
SOW	[SOW-67]	The Contractor SHALL have completed the OSA Test Cases and have received the approval by the Purchaser			
SOW	[SOW-68]	The Contractor SHALL note that system implementation activities in the operational environment SHALL NOT start until the Deployment Authorization milestone is approved by the Purchaser.			
SOW	[SOW-69]	During the event the Contractor SHALL collect from the PURCHASER assessment inputs based on Table 9 The DA Success Criteria and upon conclusion of the DA the Contractor SHALL produce a report and make it available to the Purchaser at most (1) week after the DA.			
SOW	[SOW-70]	The Contractor SHALL install, test and activate all the IEG-C components for the first operational IEG-C (IEG-C-02, see Annex B1, page 163) at SHAPE as described and defined in SECTION 6: Integrated Logistics Support (ILS), SECTION 7: System Implementation and SECTION 8: Test, Verification, Validation (TVV).			
SOW	[SOW-71]	The Contractor SHALL have delivered all functionalities of IEG-C defined within Work Packages Scope (Annex B2)			
SOW	[SOW-72]	The Contractor SHALL have trained all required personnel according to Section 6.6: Training.			
SOW	[SOW-73]	The Contractor SHALL have provided reviewed and approved operational and maintenance documentation as described in Section 6.5 Technical Documentation and Section 15: Deliverables Outlines.			
SOW	[SOW-74]	The Contractor SHALL have satisfied the security requirements (see Section 10: Security).			
SOW	[SOW-75]	The Contractor SHALL have migrated on IEG-C all services required to support the information exchange requirements for the CIS interconnection.			
SOW	[SOW-76]	All performance and availability requirements specified in this SOW (Annex A, SRS) have been met.			
SOW	[SOW-77]	The Contractor SHALL have executed all activities required to have all IEG-C software components (including ITSM tools) on the AFPL (Approved Fielded Product List).			
SOW	[SOW-78]	The Contractor SHALL have supplied the spare parts and consumables.			
SOW	[SOW-79]	The Contractor SHALL have implemented and tested all Support Services and the ITSM Tools, covering the PSA Site (SHAPE), and obtained the Purchaser's approval.			
SOW	[SOW-80]	The Contractor SHALL have updated Product Baselines (PBL) and SHALL have provided the Operational Baseline (OBL) as described in SECTION 12: Configuration Management to reflect the actual PSA configuration			
SOW	[SOW-81]	The Contractor SHALL have provided the Configuration Management database (CMDB) in a format that is compatible with the Purchaser CMDB tools.			
SOW	[SOW-82]	The Contractor SHALL have performed the Physical Configuration Audit (PCA) and Functional Configuration Audit (FCA), provided the audit reports and completed the corrective actions as outlined in the reports.			
SOW	[SOW-83]	The Contractor SHALL have executed all agreed test cases, and all tests SHALL have a status "PASS", as described in 8.5 TVV Events and results.			
SOW	[SOW-84]	All observations and deficiencies from the Formal Test Phases SHALL be handled following the Defect Management Process and be satisfactory resolved by the Contractor before awarding PSA.			
SOW	[SOW-85]	In addition to the requirements set below, the Mons site will have to achieve the requirements as set below in 3.12 Site Acceptance and SECTION 10: Security Accreditation.			
SOW	[SOW-86]	During the event the Contractor SHALL collect from the PURCHASER assessment inputs based on Table 10 PSA success criteria and upon conclusion of the PSA the Contractor SHALL produce a report and make it available to the Purchaser at most (1) week after the PSA.			

SOW	[SOW-87]	Between PSA and FSA milestones, the Contractor may propose an activation per site. In such a case, the Contractor SHALL comply with the requirements of this section in order to reach activation for a site.			
SOW	[SOW-88]	All the PSA-related requirements SHALL still be met by the Contractor.			
SOW	[SOW-89]	The Contractor SHALL have implemented the site in accordance with SECTION 6: Integrated Logistics Support (ILS), SECTION 7: System Implementation SECTION 8: Test, Verification, Validation (TVV), SECTION 9: Site Surveys and SECTION 15: Deliverables Outlines SHALL have delivered the associated documentation.			
SOW	[SOW-90]	The Contractor SHALL have installed, tested and activated the IEG-C(s) at the site.			
SOW	[SOW-91]	The Contractor SHALL have migrated on IEG-C all services required to support the information exchange requirements for the CIS interconnection(s).			
SOW	[SOW-92]	All performance and availability requirements specified in this SOW SHALL have been met by the Contractor.			
SOW	[SOW-93]	The Contractor SHALL train all required personnel according to Section 6.6: Training.			
SOW	[SOW-94]	The Contractor SHALL have supplied the spare parts and consumables.			
SOW	[SOW-95]	The Support Services SHALL have been updated as required.			
SOW	[SOW-96]	The Contractor SHALL have executed all agreed test cases, and all tests SHALL have a status “PASS” , as described in 8.5 TVV Events and results.			
SOW	[SOW-97]	The Contractor SHALL have provided the Operational Baseline (OBL) as described in SECTION 12: Configuration Management to reflect the actual Site configuration.			
SOW	[SOW-98]	The Contractor SHALL complete and receive approval by the Security Accreditation Authority (SAA) of the Security Accreditation Documentation (see para: 10.3), including all the localised versions of documents, for the site.			
SOW	[SOW-99]	The Contractor SHALL conduct OT&E as defined in Sections SECTION 7 and SECTION 8.			
SOW	[SOW-100]	The Operational Acceptance Criteria (OAC) that apply to this SOW and have been included in Annex A (SRS) have been successfully implemented or achieved.			
SOW	[SOW-101]	The achievement of the OT&E milestone SHALL be subject to the Purchaser acceptance.			
SOW	[SOW-102]	All PSA milestone requirements (see par.3.10) as well as Site Activation milestone requirements (see par.3.12: Site Acceptance) SHALL be met by the Contractor for all the sites to be implemented under this contract.			
SOW	[SOW-103]	The Contractor SHALL execute all implementation activities according to SECTION 3 at all the sites to be implemented under this contract.			
SOW	[SOW-104]	The Contractor SHALL install the most recent version of implemented IEG-C.			
SOW	[SOW-105]	The centralised management and control of the IEG-C SHALL be fully implemented by the Contractor according to the requirements specified in this SOW.			
SOW	[SOW-106]	The Contractor SHALL deliver a complete and updated set of documents (e.g. Functional Baseline, Product baseline, Operational baseline)			
SOW	[SOW-107]	The Contractor SHALL have provided the Configuration Management database (CMDB) in a format that is compatible with the Purchaser CMDB tools.			
SOW	[SOW-108]	The Contractor SHALL activate Support Services at all the FSA Sites.			
SOW	[SOW-109]	The Contractor SHALL have executed all agreed test cases, and all tests SHALL have a status “PASS”.			
SOW	[SOW-110]	The Contractor SHALL complete and receive approval by the SAA of the Security Accreditation Documentation (para: 10.3), including all the localised versions of documents (para: 10.2: Security Accreditation Authority (SAA)), for all the FSA sites.			
SOW	[SOW-111]	The Contractor SHALL deliver all deliverables (SECTION 15), and conducted all activities, as specified in this Contract.			
SOW	[SOW-112]	The Contractor SHALL close to the satisfaction of the Purchaser all outstanding issues, failures, and deficiencies.			
SOW	[SOW-113]	During the event the Contractor SHALL collect from the PURCHASER assessment inputs based on and upon conclusion of the FSA the Contractor SHALL produce a report and make it available to the Purchaser at most (1) week after the FSA.			

SOW	[SOW-114]	The Contractor SHALL at all times ensure that: o Adequate resources are applied to all activities undertaken under the contract; o Milestones are identified and achieved in a timely manner; o The project status information is comprehensively reported to the Purchaser in a timely manner; o Configuration Management baselines are established and maintained throughout the project lifecycle; o All risks (Purchaser and Contractor risks) to project achievement are identified and managed; o Professional standards of project activities and deliverables through the application of QA techniques are applied; o Due account is taken of Purchaser Furnished Information including Process Management Directives.			
SOW	[SOW-115]	The Contractor SHALL acknowledge email receipt and answer email received from NATO project team members (see para: 4.3 Project Management Organization) within 3 business days.			
SOW	[SOW-116]	The Contractor SHALL use PRINCE2 or an equivalent PM standard for the direction, governance and management activities for the entire project. If an equivalent PM standard is used, the Contractor SHALL prove that it at minimum meets all requirements stated in this section.			
SOW	[SOW-117]	The Contractor SHALL be agile in the approach for the product delivery activities within each release and by doing so SHALL enable: o All SOW requirements are met o Detailed planning and progress tracking for the short horizon (time-boxed) activities o Re-planning and reviewing activities at frequent intervals o Product deliverables breakdown and continuous (re)prioritization o Iterative development and incremental delivery via product releases o Team collaboration, rich communication, self-organisation, transparency and customer-focus o A test-driven approach utilising frequent and comprehensive testing activities using testing automation to the greatest possible extent (target 100%) o Progress Reporting with Earned Value Management (EVM)			
SOW	[SOW-118]	The Contractor SHALL define and describe its implementation of the required PM approach so that at minimum it shows a clear and consistent exchange of information between the Project team and minimal duplication of information and project management activities. For example:			
SOW	[SOW-119]	Project Master Schedule (PMS; i.e., Gantt chart) SHALL be used for higher level project planning and milestones tracking but should be regularly fed by information from Product Delivery Reviews.			
SOW	[SOW-120]	Project Status Report (PSR) SHALL include inputs about delivery progress, issues and risks taken from Product Delivery Reviews and meeting.			
SOW	[SOW-121]	The Contractor SHALL provide a Project Implementation Plan (PIP), which wil describe how the Contractor will implement the Project.			
SOW	[SOW-122]	[Reserved]			
SOW	[SOW-123]	[Reserved]			
SOW	[SOW-124]	The Contractor SHALL identify all major Contractor organizational units and any Sub-Contractors involved in the implementation of the IEG-C and a description of the portion of the overall effort or deliverable item for which they are responsible.			
SOW	[SOW-125]	The Contractor SHALL establish and maintain a Project Management Office (PMO) to perform and manage all efforts necessary to discharge all his responsibilities under this Contract.			
SOW	[SOW-126]	The Contractor SHALL also provide all necessary manpower and resources to conduct and support the management and administration of operations in order to meet the objectives of the project, including taking all reasonable steps to ensure continuity of personnel assigned to work on this project.			
SOW	[SOW-127]	The Contractor SHALL designate one or more Senior Engineer(s) as Team Managers throughout the performance of the Contract. Team Manager SHALL design, coordinate and lead the process of product delivery within the defined Product Delivery Team(s) making sure product requirements are met within given timelines and quality criteria. Team manager organizes and facilitates all Product Delivery Meetings (PDM). Team manager SHALL report and take direction from the Contractor Project Manager. See SECTION 13 for labour category requirements.			

SOW	[SOW-128]	The Contractor SHALL designate a Field Engineer to serve as the Service Direction Manager throughout the performance of the Contract. See SECTION 13 for labour category requirements.			
SOW	[SOW-129]	The Contractor SHALL designate an Engineer to serve as QAM throughout the performance of the Contract until project completion. See SECTION 13 for labour category requirements.			
SOW	[SOW-130]	The Contractor SHALL designate a Senior Engineer to serve as ILS, Change and Configuration Manager throughout the performance of the Contract, including the Operation and Maintenance (O&M) Phase. See SECTION 13 for labour category requirements.			
SOW	[SOW-131]	In order to facilitate communication and effectiveness, the Contractor SHALL locate the Core Team (i.e., Project Manager and Technical Lead) close to the Purchaser premises.			
SOW	[SOW-132]	The Contractor's team SHALL be available during EU time zone working hours (8:30 - 17:30 Monday-Thursday, and 8:30 - 16:30 on Fridays).			
SOW	[SOW-133]	The Contractor SHALL designate a Project Manager (Contractor PM), who will direct and co-ordinate the activities of the Contractor's project team. The Project Manager SHALL be the Contractor's primary contact for the Purchaser Project Manager and SHALL conduct all major project design, test, and review meetings. See SECTION 13 for labour category requirements.			
SOW	[SOW-134]	The Contractor SHALL designate a Senior System Engineer as the Technical Lead throughout the performance of the Contract. The Technical Lead SHALL lead the analysis, design, integration, transition into operations and follow-on enhancement efforts of the Contractor. See SECTION 13 for labour category requirements.			
SOW	[SOW-135]	The Contractor SHALL designate a Senior Test Engineer to serve as the Test Director for all test activities conducted under this Contract. See SECTION 13 for labour category requirements.			
SOW	[SOW-136]	The Contractor SHALL establish and maintain a Project Overview			
SOW	[SOW-137]	The Contractor SHALL establish and maintain a PBS, which SHALL: o Identify all products and shall distinguish between management products and specialist products. o Include a hierarchical diagram of all the products (management products and specialist products), having at its topmost product the final product of the overall project, i.e., the IEG-C System. o Describe each product (management products and specialist products) including its quality requirements. The product descriptions shall address sufficient detail to permit management assessment of progress.			
SOW	[SOW-138]	The Contractor SHALL establish and maintain a PFD, which SHALL sequence all products in their logical order of creation.			
SOW	[SOW-139]	The Contractor SHALL establish and maintain a PMP which shall describe how the Contractor will implement the totality of the project as specified in this SOW, including details of the project control that will be applied.			
SOW	[SOW-140]	The Contractor's PMP SHALL cover all aspects of the project implementation including its management structure and project management processes, personnel assignments, external relationships necessary to provide the capability as required by this Contract.			
SOW	[SOW-141]	The Contractor's PMP SHALL be sufficiently detailed to ensure that the Purchaser is able to assess the Contractor plans with insight into the Contractor’s plans, capabilities, and ability to satisfactorily implement the entire project in conformance with the requirements as specified in this SOW.			
SOW	[SOW-142]	The Contractor's PMP SHALL follow the outline recommended in this SOW (see SECTION 15.9).			
SOW	[SOW-143]	The Contractor's PMP SHALL be provided to the Purchaser for acceptance.			
SOW	[SOW-144]	Contractor SHALL develop the Contractor WBS to the level needed for adequate management and control of the contractual effort. A single WBS should be used for planning, managing, and reporting. o Contractor SHALL perform the contract technical effort using a guidelines-compliant EVM (EVM PMI standard) that correlates cost and schedule performance with technical progress. o Progress and problems SHALL be presented and discussed in periodic program management reviews. Technical issues SHALL be covered in terms of performance goals, exit criteria, schedule progress, risk, and cost impact. o The WBS SHALL include designation of critical subcontractors, by name, for EVM compliance and validation or flow down of EVM compliance to these subcontractors.			

SOW	[SOW-145]	The Contractor SHALL establish and maintain a PMS which SHALL: o Contain all Contract events and milestones o Correlate with the products defined in the PBS and sequentially ordered in the PFD o Incorporate the WBS o Be provided in Microsoft Project format o Identify the critical path for the overall project o Identify the start and finish dates, duration, predecessors, constraints (as necessary) and the total slack of each task o Identify key resources needed for each task completion o Identify the main project milestones (see) and intermediate milestones as required o Identify the "physical" progress for each task o Identify the applicable baseline, and shall show progress against the baseline o Minimise the use of constraints and absolute dates o Provide network, milestone, Gantt and Tracking Gantt views o Identify the main deliverables.			
SOW	[SOW-146]	The Contractor SHALL provide the PMS to the Purchaser for acceptance.			
SOW	[SOW-147]	The Contractor SHALL use the PBS, the PFD and the PMS as the primary framework for Contract planning and reporting to the Purchaser.			
SOW	[SOW-148]	The Contractor SHALL establish and maintain a RMP which shall describe how the Contractor will implement the Risk Management process, with at least the following details: o Overall Risk Management approach o Key Risk Management processes o Key Risk Categories o Risk Prioritization Matrix o Risk Management roles and responsibilities o Risk Log template which shall at minimum follow the outline recommended in this SOW (see Section 15.2).			
SOW	[SOW-149]	The Contractor SHALL establish and maintain a Risk Management process for the project, described in the RMP, and compliant with [NCIA PDED 06.00.03, 2015] and NATO Risk Management Policy.			
SOW	[SOW-150]	The Contractor's Risk Management process SHALL at minimum enable and define identification of all types of risks, evaluation and prioritization of each risk, definition of proposed response strategy, owner and actions and suggested monitor and control mechanisms.			
SOW	[SOW-151]	The Contractor SHALL document and maintain status of all risks in the Risk Log (see 15.2) where he shall record and track all project risks regardless of their status.			
SOW	[SOW-152]	The Contractor SHALL update Risk Log at minimum on a monthly basis as an input for the Project Status Report (PSR).			
SOW	[SOW-153]	The Contractor SHALL add to the Risk Log additional risks identified by the Purchaser.			
SOW	[SOW-154]	Upon Purchaser request, the Contractor SHALL deliver the Risk Log to the Purchaser, throughout the duration of the Contract.			
SOW	[SOW-155]	The Contractor SHALL establish and maintain a process for identifying, tracking, reviewing, reporting, and resolving all project issues.			
SOW	[SOW-156]	The Contractor SHALL describe the Issue Management Process in the CMP (see section 18.3).			
SOW	[SOW-157]	The Contractor SHALL develop and maintain an Issue Log (see Section 21.3) where he SHALL record and track all project issues regardless of their status.			
SOW	[SOW-158]	The Contractor SHALL include the Issue Log in the Configuration Management process and keep it under configuration control and in the Configuration Management Database (CMDB).			
SOW	[SOW-159]	The Contractor SHALL update Issue Log at minimum on a monthly basis as an input for the PSR.			
SOW	[SOW-160]	The Contractor SHALL add to the Issue Log additional issues identified by the Purchaser.			
SOW	[SOW-161]	Upon Purchaser request, the Contractor SHALL deliver the Issue Log to the Purchaser, throughout the duration of the Contract.			
SOW	[SOW-162]	The Contractor SHALL implement a QA and QC program as described in SECTION 17 SECTION 12 of this SOW.			
SOW	[SOW-163]	The Contractor SHALL deliver and maintain a Quality Assurance Plan as detailed in SECTION 11 of this SOW.			

SOW	[SOW-164]	The Contractor SHALL fully support IV&V activities and in particular: o Host inspection visits o Make himself available for answering questions and furnishing information related to the project o Allow inspection and monitoring of testing activities o Allow inspection and monitoring of Contractor's processes applicable to this project o Allow execution of independent testing activities.			
SOW	[SOW-165]	The Contractor SHALL provide, no later than the third working day of each month, a PSR. The Contractor's PSR SHALL be a monthly document.			
SOW	[SOW-166]	The Contractor's PSR SHALL at minimum summarise completed, ongoing, and upcoming activities, as well as attached updated PMS, Risk and Issue Log.			
SOW	[SOW-167]	The Contractor SHALL issue answers to Purchaser provided comments within one week after their receipt. No comment received within that timeframe means that the Contractor agrees to the comments issued by the Purchaser.			
SOW	[SOW-168]	The Contractor SHALL take meeting minutes, submit them in draft version to the Purchaser for approval within 2 working days of the meeting. The minutes SHALL be submitted to an accelerated review cycle at Purchaser's discretion.			
SOW	[SOW-169]	The participants and mainly the Contractor's representatives SHALL NOT regard these minutes as a mechanism to change the terms, conditions or specifications of the Contract nor as a vehicle to alter the design or configuration of equipment or systems. Any such changes SHALL only be made by authorised mechanisms as set forth in the Contract.			
SOW	[SOW-170]	The Contractor SHALL provide any documentation (even in draft format), that may be useful to the Purchaser in preparing for meetings and ensuring efficient discussions during the meetings no later than 2 working days before the meeting.			
SOW	[SOW-171]	The Contractor SHALL coordinate and hold PRM with the Purchaser at major milestones (listed in 3.1.2) throughout the Contract period of performance, as follows (-/+ 2 weeks around the date provided below): o PRM#1 focused on IEG-C design at EDC+5 o PRM#2 focused on Factory Tests and Accreditation at EDC+9 o PRM#3 focused on Provisional System Acceptance and the IEG-C system going live o PRM#4 focused on Final System acceptance and closing the project			
SOW	[SOW-172]	The Contractor SHALL provide an updated PSR, not older than 5 working days, as a base document for the PRM as sent to all PRM participants at least 2 business days in advance.			
SOW	[SOW-173]	At each PRM, the Contractor SHALL provide the status of all on-going tasks, the status of the Contract deliverables, identify any changes to the PMP, PMS, SIP, ILS Plan (ILSP), QAP, Issue Log, Change Requests document, Off-specifications document, baselines and Risk Log, and identify any problems.			
SOW	[SOW-174]	The Contractor SHALL address and discuss key project issues, risks and events with the Purchaser Project Manager promptly, and SHALL not postpone it until the next PRM.			
SOW	[SOW-175]	The Contractor will provide minutes of the meeting. The Minutes shall include: o Date, place, and time of the meeting: o Purpose of the meeting; o Name of participants; o Approval of previous meeting's minutes and all resolutions; o Record of principle points discussed, action taken, and decisions made			
SOW	[SOW-176]	The Contractor SHALL organize PDMs.			
SOW	[SOW-177]	The Contractor's PDMs SHALL at minimum cover the following activities: o Product Delivery Planning meeting with frequency of minimum 1 per month o Product Delivery Review meeting with frequency of minimum 1 per month o Product Delivery Progress Meeting with frequency of minimum every 2 working days			
SOW	[SOW-178]	All PDMs SHALL be organized and run by Team Manager or Tech Lead appointed by the Contractor.			

SOW	[SOW-179]	The Contractor SHALL record all outputs from all PDMs in a product delivery toolset chosen, implemented and hosted by the Contractor.			
SOW	[SOW-180]	The Contractor SHALL ensure Purchasers access to the abovementioned product delivery toolset.			
SOW	[SOW-181]	The Contractor SHALL report key outputs from PDMs such as delivery progress information (e.g., product backlog status, key test results, burn down / burnup charts) as well as key changes, issues and risks to the Contractor Project Manager who SHALL integrate that information in the PSR.			
SOW	[SOW-182]	The Contractor's Project Manager SHALL provide inputs to and attend IPMT meetings as requested by the Purchaser Project Manager.			
SOW	[SOW-183]	For daily/regular contact the Contractor SHALL designate Security SMEs as points of contact for security accreditation and security-related issues. .			
SOW	[SOW-184]	The Contractor SHALL maintain a NATO RESTRICTED Project Portal (provided by the Purchaser) on which all relevant (classified up to and including NATO RESTRICTED) CO-14314-IEG-C project documentation and datasets shall be maintained. This Project Portal is created on the NATO RESTRICTED network at NCIA by the Purchaser, and will be accessed by the Contractor using the Purchaser provided REACH laptop(s) (See Annex B of the Contract Special Provisions) or any other approved device/mechanism for the exchange of NATO RESTRICTED information. Accreditation related documentation SHALL also be stored and referenced thereafter, in the NCIA Security Accreditation Portal.			
SOW	[SOW-185]	The Contractor SHALL maintain on this website all unclassified documents, as soon as they are submitted in draft version to the Purchaser. This includes all project deliverables, presentation materials from all meetings, as well as the Contract SOW and SRS, and all applicable documents. More generally, the website SHALL include any document as deemed necessary by the Purchaser.			
SOW	[SOW-186]	The Contractor SHALL identify all relevant classified documents on the Project Website, by title, unless a title itself is classified and SHALL state from where the classified document can be obtained.			
SOW	[SOW-187]	The Contractor SHALL submit all documentation in electronic format to the Purchaser for review and comments as applicable.			
SOW	[SOW-188]	The Contractor SHALL not provide any Contractual documentation in a partial or gradual manner.			
SOW	[SOW-189]	The Contractor SHALL ensure that any documentation delivered to the Purchaser has been properly reviewed according to Contractor quality management process, utilizing the Project Portal and other shared resources, and minimizing use of personal storage and email, to the extent possible.			
SOW	[SOW-190]	The Contractor SHALL provide a first version of each deliverable for Purchaser review. The first version SHALL be substantially complete and correct.			
SOW	[SOW-191]	The Contractor SHALL not rely on the Purchaser review to fill in deficiencies or obtain missing Purchaser information.			
SOW	[SOW-192]	The Contractor SHALL resubmit the document as a revised version addressing the Purchaser's comments within 2 (two) weeks after receipt.			
SOW	[SOW-193]	The Contractor SHALL provide an updated version of the document within two weeks of receipt of the Purchaser's comments on the revised version.			
SOW	[SOW-194]	If the document is included as part of the ABL or PBL, the Contractor SHALL remain responsible for updating the document as required in the course of the project (to correct errors, inconsistencies, omissions, etc. and to reflect changes in the system design, system implementation, support arrangements) as part of its Configuration Management tasks.			
SOW	[SOW-195]	The Contractor SHALL be able to adapt the IEG-C to accommodate this additional information.			
SOW	[SOW-196]	The Contractor SHALL incorporate in his activities the integration, performance, and schedule considerations related to the co-ordination of the IEG-C with the other Purchaser systems to be interfaced with it throughout the duration of the project.			
SOW	[SOW-197]	The Contractor SHALL identify any documents, meeting minutes, or other information from these projects required to maintain an effective co-ordination process.			
SOW	[SOW-198]	The Contractor SHALL include into Project Communication Plan (part of PMP) activities clearly identifying his proactive approach with regards to the coordination with other related NATO projects.			
SOW	[SOW-199]	As a Project-level communication activity, the Contractor SHALL provide an IEG-C Information Sheet of maximum 2 pages providing an overview of the IEG-C system, its functions, external interfaces and major components, and its projected installation schedule.			
SOW	[SOW-200]	The Contractor SHALL be responsible for the overall design, integration, obtaining security accreditation and system engineering of the IEG-C throughout the Contract period of performance.			
SOW	[SOW-201]	The Contractor SHALL develop the IEG-C System Design Specification (SDS) based on an analysis of the Purchaser's requirements.			

SOW	[SOW-202]	The Contractor SHALL integrate all necessary components to establish the IEG-C Product Baseline, and plan and execute a series of tests to confirm that this baseline meets its functional and non-functional requirements (portability, maintainability, security, reliability, usability, compatibility, performance, functional).			
SOW	[SOW-203]	The Contractor SHALL perform the activities described in this section considering that the IEG-C will integrate with a wide variety of NATO activities and systems (e.g., Core Services, Functional Area Services (FAS)).			
SOW	[SOW-204]	The Contractor SHALL be responsible for integration of the IEG-C System. This means both the integration of the various products that constitute the IEG-C System and the integration of the IEG-C System with other NATO systems.			
SOW	[SOW-205]	The Contractor SHALL make use of NCIA testbed (Annex B1) to perform the integration or more generally to conduct tests, and in particular the following Milestone events: o Factory Acceptance Test (FAT at EDC+9MO) (see Section 3.5.4) at the Contractor premises if the contractor has chosen to develop on their own premises; or the Purchaser's Development and Integration Testing Environment (see Section 5.1.1.2) if the Contractor has chosen to develop on the Purchaser's Development and Integration Testing Environment. o Integration and Interoperability tests (SIT milestone at EDC+17mo) related to the integration of the IEG-C system with other NATO systems, at the Purchaser's Development and Integration Testing Environment. o System Acceptance Test (SAT) and User Acceptance Test (UAT) for the Formal Verification and Validation and the execution of tests in support of NATO's change process with the objective to achieve Deployment Authorization, at the NATO Enterprise Reference System (see Section 5.1.1.7).			
SOW	[SOW-206]	The Contractor SHALL deliver and install the IEG-C Integration Test System with all its components as defined in ANNEX B, in compliance with the processes described in SECTION 13 as a virtualized system and SHALL integrate it within the contractor provided Development and Integration Test Environment.			
SOW	[SOW-207]	The Contractor SHALL provide the operating systems and any other COTS software needed by the IEG-C Integration Test System with the necessary Original Equipment Manufacturer's manuals and licenses unless agreed to be provided by the Purchaser.			
SOW	[SOW-208]	The Contractor SHALL install the COTS software on the IEG-C Integration Test System and apply the necessary configuration.			
SOW	[SOW-209]	The Contractor SHALL implement a procedure to ensure that the IEG-C Integration Test System is representative of the actual operational system, in particular in terms of design and configuration, and software versions.			
SOW	[SOW-210]	The Contractor SHALL establish and update the IEG-C Integration Test System on the Purchaser prepared Development and Integration Test Environment prior to the relevant events.			
SOW	[SOW-211]	The Contractor SHALL update the IEG-C Integration Test System with each new release until FSA.			
SOW	[SOW-212]	The Contractor SHALL demonstrate how the Purchaser will have to make use of the IEG-C Integration Test System to adapt any existing software, scripts, reports etc. to changing requirements (this encompasses both development and testing activities).			
SOW	[SOW-213]	The Contractor SHALL deliver hardware components for elements of the IEG-C Reference System that cannot be virtualized.			
SOW	[SOW-214]	The Contractor SHALL deliver and install the IEG-C Reference System with all its components as defined in ANNEX B, in compliance with the processes described in SECTION 13, and SHALL integrate it within the Contractor provided NATO Enterprise Reference System.			
SOW	[SOW-215]	The Contractor SHALL provide the operating systems and any other COTS software needed by the IEG-C Reference System with the necessary Original Equipment Manufacturer's manuals and licenses unless agreed to be provided by the Purchaser.			
SOW	[SOW-216]	The Contractor SHALL install the COTS software on the IEG-C Reference System and apply the necessary configuration.			
SOW	[SOW-217]	The Contractor SHALL implement a procedure to ensure that the IEG-C Reference System is representative of the actual operational system, in particular in terms of design and configuration, performance, security settings, and software versions.			
SOW	[SOW-218]	The Contractor SHALL demonstrate how the Purchaser will have to make use of the IEG-C Reference System to adapt any existing software, scripts, reports etc. to changing requirements (this encompasses both development and testing activities).			
SOW	[SOW-219]	The Contractor SHALL establish and update the IEG-C Reference System on the Purchaser prepared Development and Integration Test Environment prior to the relevant events.			
SOW	[SOW-220]	The Contractor SHALL update the IEG-C Reference System with each new release until FSA.			
SOW	[SOW-221]	The Contractor SHALL deliver and activate the IEG-C Reference System. The Contractor SHALL deliver all documents as required in this section for the Reference System (e.g., SIP, accreditation documents, etc.).			

SOW	[SOW-222]	The Contractor SHALL conduct a workshop (at a Purchaser-provided facility) to orient the IEG-C Platform Administrators and other stakeholders (Contractor proposes Purchaser decision) on the overall system design and capabilities. As part of this workshop, the Contractor SHALL: o deliver overview briefings on the anticipated IEG-C system, and lead question and answer sessions with the attendees; o provide visuals, models, demonstration as necessary; o provide information about the anticipated IEG-C System Implementation; o provide information about how the System Design fully meets the requirements specified in this SOW and SRS; o provide an overall description of the external interfaces; o provide an overall description of the ILS concept and strategy; o Provide an overall description of Configuration Management and Quality concept and strategy. o Collect any necessary information from the IEG-C Administrators, CIS Security Administrators and other stakeholders in order to perform the design activities. As required, the Contractor SHALL conduct further dialogue with the IEG-C Administrators, CIS Security Administrators and other stakeholders.			
SOW	[SOW-223]	The Contractor SHALL propose the event date minimum 2 months in advance to allow the coordination time with various stakeholders. The Contractor SHALL provide the proposed content for the workshop including schedule, coverage, content, presentation and the information for Purchaser approval minimum 4 weeks prior to the event.			
SOW	[SOW-224]	The Contractor SHALL review the IEG-C SRS and all applicable documents, meet and communicate with NATO SMEs as necessary, and present its findings in terms of proposed changes to the SRS based on system cost, schedule, or performance impacts.			
SOW	[SOW-225]	The Contractor SHALL also identify any inconsistencies within the requirements. Any inconsistencies not identified by the requirements review will not be accepted later as the basis for a change with cost impact.			
SOW	[SOW-226]	The Contractor SHALL host and conduct a System Requirements Review (SRR at EDC+2MO) to present and discuss its findings and proposed changes to the requirement baseline for the design and integration of the IEG-C project. The purpose of this review is to agree upon the requirement baseline for the design and integration of the IEG-C system.			
SOW	[SOW-227]	The contractor SHALL produce and provide a set of minutes that accurately reflect the discussions taken during the SSR meeting and provide them to the purchaser within 1 week of the meeting.			
SOW	[SOW-228]	Upon completion of the SRR, the Contractor SHALL identify any proposed changes to System Requirements Specification in the form of one or more Change Requests (i.e. ECPs). These Change Requests SHALL be addressed according to the processes implemented by the Contractor to meet the requirements of 12.6 and of 15.5 Change Request.			
SOW	[SOW-229]	The Contractor SHALL use the updated FBL as the basis for the IEG-C system design and subsequent activities.			
SOW	[SOW-230]	The Contractor SHALL review the Purchaser-provided provided IEG-C Target Architecture [NCIA TR/2016/NSE010871/01, 2017].			
SOW	[SOW-231]	The Contractor SHALL consider this Target Architecture as a document for information which should be helpful to conduct its design activities. Therefore, the Contractor SHALL NOT consider the Target Architecture as a binding document.			
SOW	[SOW-232]	The Contractor SHALL conduct the necessary Design Activities and develop its own complete design of the IEG-C at the Preliminary and Critical levels, including all interfaces to other systems to meet the SRS.			
SOW	[SOW-233]	The Contractor SHALL keep the system design documentation package (including security accreditation documentation) up to date throughout project execution, in particular as a result from the site surveys and/or in order to obtain the security accreditation.			
SOW	[SOW-234]	The Contractor’s IEG-C System Design SHALL cover all sites identified for this project.			
SOW	[SOW-235]	The Contractor’s IEG-C architecture SHALL be designed so that it can be reused for other security classification levels (in any case, the system will be installed and operated at System High/NS mode of operation).			
SOW	[SOW-236]	The Contractor’s IEG-C architecture SHALL be designed to be modular design, allowing for future extension and enhancements.			
SOW	[SOW-237]	The Contractor's IEG-C architecture SHALL be designed so that it can be reused in the deployed environment.			
SOW	[SOW-238]	The Contractor SHALL agree coding syntax(es) with the Purchaser during the Design Stage.			
SOW	[SOW-239]	The IEG-C Contractor SHALL ensure that the design is compliant with and covers the System Operations Processes.			

SOW	[SOW-240]	The Contractor SHALL establish, deliver and maintain the IEG-C System Design Documentation Package, comprising of: o The System Design Specification (SDS), o The Interface Control Document (ICD), o The Security Accreditation Documentation Package o The Master Test Plan (MTP), and o The Requirements Traceability Matrix (RTM).			
SOW	[SOW-241]	The duration of the review cycle for the IEG-C System Design Documentation Package SHALL be 4 (four) weeks.			
SOW	[SOW-242]	The Contractor SHALL prove the design through the regime of testing set forth in the Contract and the Contractor SHALL be responsible in the event that the system proves deficient in meeting the Contractual requirements.			
SOW	[SOW-243]	As part of the Configuration Management activities, and like any other management product or specialist product, the Contractor SHALL update the System Design Documentation Package to reflect changes, at least at each of the following major milestones: a new design review, the start of a test phase, the completion of each tests activities, the start of the deployment, PSA, FSA.			
SOW	[SOW-244]	The Contractor SHALL ensure that in order to maintain clear consistency throughout all documents in the System Design Documentation Package, any update of any of the documents comprised in the System Design Documentation Package SHALL result in re-delivery of a new version of the complete System Design Documentation Package.			
SOW	[SOW-245]	The Contractor's SDS SHALL describe the IEG-C System to a level of detail that is sufficient for the Purchaser to be able to understand how the requirements in the SRS and the security requirements (see ANNEX A) are implemented.			
SOW	[SOW-246]	In particular, the Contractor's IEG-C SDS SHALL address the IEG-C Operational Requirements (see SRS).			
SOW	[SOW-247]	The Contractor's IEG-C SDS SHALL be developed as per the detailed contents indicated in section 21.6.			
SOW	[SOW-248]	~~The Contractor SHALL document, as specific annexes to the ICD:~~ ~~o Each direct interface between the IEG-C and NEDS to include detailed descriptions of any "configuration settings" and agreements to enable synchronisation between IEG-C and NEDS.~~ ~~o Each direct interface between the IEG-C and other systems (e.g., AIFS, E-NPKI)~~ ~~o Each interface between the IEG-C subordinate or superior IEG-C components~~ ~~o Each interface between the IEG-C and end-entity users and devices SHALL be documented~~			
SOW	[SOW-249]	Where work was conducted by the Contractor under this Contract to document the design of any system to be interfaced to the IEG-C project, the results of that work SHALL be included in the relevant annex of the ICD.			
SOW	[SOW-250]	The Contractor SHALL develop the ICD in accordance with the template provided by the Purchaser.			
SOW	[SOW-251]	The Contractor SHALL ensure that the Security Accreditation Documentation Package comprises all documentation mentioned in Section 10.3.			
SOW	[SOW-252]	The Contractor SHALL develop and maintain a RTM that establishes a complete cross-reference between on the one hand the requirements stated in the SRS, System Security Requirements Statement (SSRS), and on the other hand the detailed contents of the SDS in terms of SDS statements and lowest-level CIs.			
SOW	[SOW-253]	The Disaster Recovery Plan & Procedures and the Backup Plan & Procedures prepared by the Contractor SHALL address the best practices developed by the vendors of the system components, including security best practices.			
SOW	[SOW-254]	The Disaster Recovery Plan & Procedures prepared by the Contractor SHALL address all possible scenarios and corresponding actions, including security.			
SOW	[SOW-255]	The Disaster Recovery Plan & Procedures prepared by the Contractor SHALL align with the site-specific Disaster Recovery Plan & Procedures, including those defined in the ITM Joining Instructions.			
SOW	[SOW-256]	The Backup Plan & Procedures prepared by the Contractor SHALL align with the site-specific Backup Plan & Procedures, including those defined in the ITM Joining Instructions.			

SOW	[SOW-257]	As a minimum, the Disaster Recovery Plan and Procedures prepared by the Contractor SHALL address the following scenarios: o Recovery of an entire IEG-C; o Transfer of an IEG-C service from one platform to another. o The Contractor SHALL define for every IEG-C component: o Storage capacity for back up o Type of storage to use o Back up frequency o Type of back up (full or incremental) o Level of information to back up			
SOW	[SOW-258]	The Disaster Recovery Plans & Procedures prepared by the Contractor SHALL clearly distinguish between service restoration and data restoration, and SHALL include a disaster recovery kit.			
SOW	[SOW-259]	The Contractor SHALL deliver the disaster recovery kit which SHALL contain distribution media for all software (including versions, upgrades/updates, patches and hot-fixes) to restore an IEG-C Element from “bare metal”, in accordance with site-specific Disaster Recovery plans.			
SOW	[SOW-260]	The Contractor SHALL deliver the disaster recovery kit that includes a full, customized, installation plan that covers all steps (including Operation System (OS) installation) to build and configure each of the IEG-C components.			
SOW	[SOW-261]	The Contractor SHALL ensure that Volume Shadow copy service SHALL be used to optimize the backup/recovery process where appropriate.			
SOW	[SOW-262]	The Contractor SHALL ensure that disaster recovery and back-up procedures is included in the Technical Manuals and SHALL be a dedicated section of it.			
SOW	[SOW-263]	The Contractor SHALL ensure that disaster recovery Kit is analysed in terms of ILS resources and all the necessary resources and support needed for disaster recovery is produced as required in SECTION 6 : Integrated Logistics Support (ILS) of this document.			
SOW	[SOW-264]	The Contractor SHALL conduct Design Reviews, a Preliminary Design Review (PDR at EDC+3MO) and a Critical Design Review (CDR at EDC+6MO), to present the IEG-C Design Documentation Package. The Contractor SHALL include the following areas in the Design Review: o IEG-C overall system architecture and interactions o System functionality, modularity and interfaces, breakdown into lowest-level Configuration Items (CI; see section 12.4 for CIs identification) o Off-the-shelf products to be used in the system: the Contractor SHALL identify the intended product and version, and note if any additional elements (such as macros or plug-ins) are required o Interfaces with other relevant systems (i.e., with NEDS) o System security design: Presentation of the Risk Assessment Methodology that the Contractor intends to use for the Project, Results of the Risk Analysis, Definition and implementation of the Security measures to counter the risks that will be identified in the Security Risk Assessment (SRA). This presentation SHALL be done as a separate item. o Sequence and scope of system tests of the ABL and any requirements for Purchaser support and participation o Any change request or off-specification o Any changes to the PBS and PFD o Any changes to the PMS o Cost considerations o Risk assessment of proposed changes and an update of the Risk Log and Issue Log o RTM o MTP traceable to system system/component requirements and acceptance criteria.			
SOW	[SOW-265]	The Contractor SHALL provide a Design Review Report for every Design review cycle.			
SOW	[SOW-266]	The Contractor SHALL update the Design Documentation Package as per the result of the Design Review.			
SOW	[SOW-267]	The Contractor activities and milestones related to ILS SHALL be identified and included in the PMS of the PMP.			
SOW	[SOW-268]	The Contractor SHALL use the [ALP 10-2016] and [AIA/ASD SX000i, 2016] specification as guidance when establishing and conducting the ILS Process (i.e. Integrated Logistics Support – ILS Process), in accordance with the requirements of the contract.			

SOW	[SOW-269]	The Contractor SHALL use [ADMP-1], [ADMP-2], [MIL-HDBK-338B], [MIL-HDBK-470A], [MIL-STD-1388-1A], [MIL-STD-1388-2B] and [ASD S3000L] as guidance when establishing and conducting the Logistic Support Analysis (LSA) programme, including the RAMT programme, in accordance with the requirements of the Contract.			
SOW	[SOW-270]	The Contractor SHALL provide and maintain an ILSP, tailored to the Project Program phases.			
SOW	[SOW-271]	The Contractor SHALL develop the ILSP in accordance with the requirements described in this section and cover all areas.			
SOW	[SOW-272]	The Contractor SHALL detail in the ILSP how ILS will be designed, managed, procured and provided throughout the system lifetime.			
SOW	[SOW-273]	The Contractor SHALL provide an updated version of the ILSP to the Purchaser for each milestone for Purchaser acceptance.			
SOW	[SOW-274]	The Contractor SHALL cover the following sections at minimum including the processes to perform the related activities in ILSP: o The Contractor's ILS organization, roles, responsibilities and procedures; o Maintenance Concept (Maintenance Plan, detailed Maintenance Level definitions and tasks); o Planning of supply support (System Inventory, Codification, Recommended Spare Parts and Consumables list); o Design Influence i. Reliability, Availability, Maintainability and Testability (RAMT) Programme planning, activities, processes (including testing); ii. Logistics Support Analysis planning, activities and processes; iii. Support Case planning, releases and processes. o Support and Test Equipment Lists; o Computer Resources (licences, SWDL etc.); o Manpower and Personnel Requirements; o Technical Documentation (organization, process, inputs, reviews, release schedule) o Planning of packaging, handling, storage, and transportation (PHS&T); o Planning of supply chain security. o In-Service Support Plan (as an annex)			
SOW	[SOW-275]	The Contractor SHALL maintain and update the ILSP as required to reflect changes in the Project Baselines, in the SOW, or in support arrangements for any IEG-C System CIs.			
SOW	[SOW-276]	The Contractor SHALL provide an In Service Support Plan (ISSP) as an annex to the ILSP and SHALL cover the following topics at minimum with practical instructions: o the Contractor's Support organization, roles, responsibilities, processes and procedures (between PSA and FSA; and during warranty); o description of the system of interest (SOI) in scope of integrated support, o description of the integrated support concept, including the maintenance concept, warranty concept, customer support concept, service management & control concept including but not limited to the incident, problem management, release and deployment management, and configuration and change management; o description of the parties involved, their responsibilities for the various levels of support (with indication of start and end dates), interfaces, response times and POC details; o description and allocation of operation, SM&C and corrective and preventive maintenance tasks required to operate and maintain the system; o description of the Sustainability measures (obsolescence management, failure reporting, performance monitoring, reliability and availability assessment and reporting); o procedures to follow when any part of the system fails; response times for analyses and resolution by the Contractor, o comprehensive lists of all available spares, consumables, software licenses (SWDL), support software tools, COTS documentation, technical documentation, training documentation and manuals.			
SOW	[SOW-277]	The Contractor SHALL provide the latest ISSP as part of PSA (EDC+20mo) and FSA (EDC+27mo) milestone achievement.			
SOW	[SOW-278]	As an Annex of the ILSP and in accordance with SOW ANNEX F, the Contractor SHALL develop and maintain the IEG-C System Maintenance and Support Concept that defines the maintenance and support environment, constraints, locations, procedures, artefacts, organisation and personnel skills to maintain the Delivered baselines of the IEG-C Capability.			

SOW	[SOW-279]	The Contractor SHALL design/deliver the system/elements and the Operation/Support/Maintenance documentation, training, instructions, and resources (skills, tools/test equipment) in order to allow the Purchaser to fully operate the system, to perform Level 1, Level 2 and Level 3 Maintenance and Support from the Provisional Site Acceptance (PSA).			
SOW	[SOW-280]	Starting from PSA (EDC+20mo) and until FSA (EDC+27mo) with all the sites are completed; the Contractor SHALL be responsible for the Level 2, Level 3 and Level 4 maintenance and support activities in each activated site within the scope of the Initial Operational Support.			
SOW	[SOW-281]	Starting from FSA and until the end of warranty period, all maintenance activities beyond Purchaser capabilities/skills (as per Maintenance Concept and Contractor delivered training and documentation) required to restore the System from a critical failure SHALL be carried on by the Contractor by dedicated on-site interventions and/or off-site resolutions.			
SOW	[SOW-282]	The Contractor SHALL ensure the Maintenance and Support Concept refers to the functional and non-functional Requirements of the IEG-C System.			
SOW	[SOW-283]	The Contractor SHALL ensure the Maintenance and Support Concept defines the Maintenance and Support tasks at any level of support and at any level of maintenance.			
SOW	[SOW-284]	The Contractor SHALL ensure the Maintenance and Support Concept defines the Delivered Baselines maintenance and supply flow amongst the various NATO locations, organisations, groups, and people.			
SOW	[SOW-285]	The Contractor SHALL ensure the Maintenance and Support Concept defines and describes the Maintenance and Support process interfaces to all other processes.			
SOW	[SOW-286]	The Contractor SHALL define the 2nd and 3rd Level Support process interfaces to the other processes, including the existing NCIA Service Desk (1st Level of Support).			
SOW	[SOW-287]	The Contractor SHALL ensure the Support process interface definition includes the input and output information, its structure, the communication path (i.e., Points of Contact (POC)), the time constraints for sending and receiving information, and quality criteria to evaluate the integrity of the interface. This SHALL Include the related ITIL Processes to be tailored and detailed for the purposes of IEG-C System Support Concept.			
SOW	[SOW-288]	At each Support and Maintenance Level, the Contractor SHALL ensure the Support Concept describes the support environment, constraints, locations, procedures, artefacts, organisation and personnel.			
SOW	[SOW-289]	The Contractor SHALL ensure the procedural description includes objective(s), triggering event(s), input(s), output(s), task(s), roles and responsibilities (Responsible, Accountable, Consulted and Informed (RACI) format), constraints, exceptional case(s), and tool(s) support.			
SOW	[SOW-290]	The Contractor SHALL ensure the IEG-C System ILSP is based on the established Support Concept, approved by the Purchaser before the CDR (EDC+6MO) milestone.			
SOW	[SOW-291]	The Contractor SHALL develop its RAM Programme and perform the analysis based on the RAM metrics and requirements outlined in the SRS.			
SOW	[SOW-292]	The Contractor SHALL ensure the design of the system includes sufficient redundancy and other Reliability, Maintainability, Availability and Testability measures to ensure the RAM requirements in this Contract are achieved and attained at an optimal Total Cost of Ownership (TCO), minimising preventive maintenance, manpower requirement and usage of special-to-type tools and test equipment.			
SOW	[SOW-293]	Such measures taken to ensure fulfilment of RAM requirements and optimisation of TCO SHALL be documented in the Support Case.			
SOW	[SOW-294]	The RAM analysis SHALL clearly capture and display the RAM characteristics of each main component, aggregated up to the level of sub-system, and subsequently the entire system. System breakdown in line with the configuration item structure SHALL be used as reference to perform the analysis.			
SOW	[SOW-295]	The RAM SHALL be used to calculate and predict intrinsic availability and operational availability, as defined in SRS, for each type of subsystem, each type of node and each type of end-to-end connection.			
SOW	[SOW-296]	The RAM analysis SHALL include the reliability prediction based on the proposed design solution and created RBDs, as well as the reliability allocation model to include to trigger the design changes			
SOW	[SOW-297]	The RAM analysis SHALL include Failure Modes, Effects and Criticality Analysis (FMECA) in accordance with MIL-STD-1629A.			
SOW	[SOW-298]	The Contractor SHALL ensure that the first issue RAM analysis is performed and delivered before PDR (EDC+3MO) , updated before CDR and finally accepted at CDR (EDC+6MO), to include all relevant data to demonstrate compliance with the SRS and SOW requirements. Such data SHALL be documented in the Support Case as outlined below.			

SOW	[SOW-299]	The Contractor SHALL conduct a Logistic Support Analysis (LSA) Process, tailored to support the specific scope of the System operation activities.			
SOW	[SOW-300]	The Contractor's LSA analysis SHALL include, as a minimum: o Task Analysis for identification of operational tasks, Service Management and Control (SMC) tasks; and administration and maintenance tasks (corrective, preventive, adaptive) o Level of Repair Analysis (LORA) to determine the correct level of Support/Maintenance needed to perform each Operational and Maintenance task o Planning and execution of the O&M Procedures Verification Test with references to the Master Test Plan. o Total Cost of Ownership Analysis, which SHALL include the warranty cost and all the operational costs and all the maintenance cost for all the support and Maintenance levels for at least 5 years after FSA o Obsolescence Analysis and Management for each software and hardware CI from end of sales, end of production and end of support perspective. .			
SOW	[SOW-301]	The Contractor's analysis SHALL contain also the list of procedures needed to configure the capability for mission and/or exercise environment.			
SOW	[SOW-302]	The Contractor SHALL ensure that Operation tasks are identified through analysis of the functional and non-functional requirements of the new system taking into account mission scenarios and conditions under which the system will be operated.			
SOW	[SOW-303]	The Contractor SHALL ensure the analysis examines each system function allocated to personnel and determines what operator tasks are involved in the performance of each system function.			
SOW	[SOW-304]	The Contractor SHALL ensure that maintenance tasks are identified using the RAM data and results.			
SOW	[SOW-305]	The Contractor SHALL ensure the SMC tasks are identified through analysis of all functions related to customer support and SMC.			
SOW	[SOW-306]	For each task in Task Analysis, the Contractor SHALL determine the properties and physical resources required to execute the task. For that purpose, each task SHALL be analysed to identify and capture: o The support level to be assigned; o Location/ facility involved; o Personnel skills required; o Roles (as they are assigned in Purchaser's maintenance and support organization); o Task duration and frequency, reusing Mean Time Between Failures (MTBF) and Mean Time To Repair (MTTR) data available;			
SOW	[SOW-307]	For each task, the Contractor SHALL perform a cost calculation based on the properties and physical resource requirements of each task.			
SOW	[SOW-308]	The cost calculation SHALL provide an estimated annual cost for each task.			
SOW	[SOW-309]	The Contractor SHALL ensure the data and results of the Task Analysis are used as input to the development of technical publication (all manuals at any level of maintenance) and the development of training material.			
SOW	[SOW-310]	The Contractor SHALL document the LSA and RAM process, resourcing and organization, inputs, outputs, methodology, and timelines within ILSP.			

SOW	[SOW-311]	The Contractor SHALL develop and maintain the necessary Support Cases in which all LSA and RAM activities SHALL be documented. The Support Case SHALL include: o System description and breakdown down to lowest level of maintenance significant items (I.e. LRUs, SRUs) and in accordance with the CI structure and identifications o All COTS equipment datasheets, clearly indicating the reliability and maintainability characteristics which will be used as input for LSA and RAM. o Availability, Reliability, and Maintainability analysis modelling, calculations and results (complete set of Reliability Block Diagrams (RBDs), FMECA including a list of critical items); o Spare part calculations and modelling, o Recommended Items List (RIL) including spares, consumables, tools and test equipment with rationale and justifications, o The complete data for LSA activities and results, o The complete data set of the Task Analysis, including listings of all operation tasks, SMC tasks, administrative tasks, corrective maintenance tasks and preventive maintenance tasks; o References to the Master Test Plan and other relevant testing documentation for RAM requirements verification and validation; o The results of the Disaster Recovery Logistic Analysis. o The results from the O&M Procedures Verification Test; o The Total Cost of Ownership Analysis results o The Obsolescence Analysis results			
SOW	[SOW-312]	The Contractor's Support Case SHALL form a body of evidence, providing sufficient credibility that all LSA and RAM requirements outlined in SOW 6.4.1 and 6.4.2, and SRS have been met and providing credibility to the data used and the results achieved in all calculations and models.			
SOW	[SOW-313]	The Contractor's Support Case SHALL provide rationale and justifications for all data and formulas used in any of the calculations and models.			
SOW	[SOW-314]	The Contractor SHALL ensure that the first issue of Support Case is delivered before PDR (EDC+3MO) encompassing all the design details up to the PDR milestone, updated before CDR and accepted at CDR (EDC+6MO), to include all relevant data to demonstrate compliance with the SRS and SOW requirements.			
SOW	[SOW-315]	The Contractor SHALL provide all the technical documentation for IEG-C System.			
SOW	[SOW-316]	The Contractor SHALL ensure all the Technical Documentation is kept updated and under configuration control for the entire life cycle of the system.			
SOW	[SOW-317]	The Contractor SHALL ensure the information contained in each technical documentation is coherent with the operational configuration deployed, i.e., OBL.			
SOW	[SOW-318]	Technical documentation SHALL consists (as a minimum) of: o Training documentation o Operation and User Manuals o Maintenance Manual (including administration manuals) o OEM Manuals for Commercial-Off-The-Shelf (COTS) products o As-Built Documentation o Other project documentation as required in this SOW.			
SOW	[SOW-319]	The Contractor SHALL ensure the all activities, milestones and actors associated with the development of technical documentation are described in the ILSP.			
SOW	[SOW-320]	The Contractor SHALL ensure all technical documentation SHALL be provided in the English language.			
SOW	[SOW-321]	The Contractor SHALL provide technical documentation as required in the various Sections of this SOW.			
SOW	[SOW-322]	The Contractor SHALL ensure the Classification of Technical documentation is at the lowest level possible.			
SOW	[SOW-323]	The Contractor SHALL ensure the all documents, however short, identify the complete name and version of the software they refer to, originator, date of production, the type of document, and Configuration Management information of the document itself.			
SOW	[SOW-324]	The Contractor SHALL ensure the all documents also contain a list of those CIs (title and version identifier) that the document or parts thereof refer to.			

SOW	[SOW-325]	The Contractor SHALL submit all final and accepted versions of documentation deliverables in electronic format, as Portable Document Format (PDF).			
SOW	[SOW-326]	The Contractor SHALL submit documentation, intended for review by the Purchaser, with each modification identified through the change tracking feature or otherwise marked.			
SOW	[SOW-327]	The Contractor SHALL submit documentation, intended for review by the Purchaser, in electronic format.			
SOW	[SOW-328]	The manuals SHALL supplement the COTS O&M documentation the Contactor SHALL provide with the IEG-C System.			
SOW	[SOW-329]	The Contractor SHALL capture and document lessons learned during the System development and the System Installation.			
SOW	[SOW-330]	If activated, the Contractor SHALL provide updated technical documentation in accordance with Section 6.5 to cover the changes for each optional site and service outlined in the SSS.			
SOW	[SOW-331]	The Contractor SHALL develop, provide and maintain the System Operation Manual (SOM).			
SOW	[SOW-332]	The Contractor SHALL provide an Operation Manual that describes the complete system by the explanation of functional blocks and CIs (HW, SW).			
SOW	[SOW-333]	The Contractor SHALL provide an Operation Manual that defines the in-depth, step-by-step procedure how to operate the system and how to perform Level 1 maintenance tasks.			
SOW	[SOW-334]	The Contractor's SOM SHALL include all the possible system operations in order to safely operate and use the capability.			
SOW	[SOW-335]	The Contractor SHALL ensure the operation described in the Manual is an outcome of the Operation and maintenance Task Analysis as described in this SOW.			
SOW	[SOW-336]	The Contractor SHALL ensure that each and every procedure include as a minimum the following information: o Location/facility involved (if the operation is performed remotely, it has to be specified); o Personnel skills required; o Task duration and frequency, reusing MTBF and MTTR data available; o Manpower required; o Tools and special tools required (if any); o The steps needed to perform the operation.			
SOW	[SOW-337]	The Contractor SHALL develop, provide and maintain the System Maintenance and Administration Manual.			
SOW	[SOW-338]	The Contractor SHALL ensure the Maintenance Manual contains all possible Scheduled and Unscheduled maintenance procedures and all possible Administration procedures as requested in this SOW.			
SOW	[SOW-339]	The Contractor SHALL ensure the Maintenance Manual contains a full illustrated product breakdown list. The Contractor SHALL ensure that all CIs and all items required for maintenance are included in this full product breakdown list.			
SOW	[SOW-340]	The Contractor's Maintenance Manual SHALL provide functional descriptions and specifications, with appropriate drawings, of the mechanical, electrical, and electronic assemblies, sub-assemblies, physical and logical components, configuration files and interfaces that comprise the system.			
SOW	[SOW-341]	The Contractor's Maintenance Manual SHALL provide information, illustrations, and procedures required for: deployment, installation, configuration, provisioning, disaster recovery, backup/restore, BIT/condition monitoring, fault finding and fault isolation/ troubleshooting techniques, test remove/ replace; and check out of each hardware and software item with relevant safety instructions.			
SOW	[SOW-342]	The Contractor's Maintenance Manual SHALL provide description of all the configuration settings for the modules, services and components/ how configuring the logging and uses of performance counters/ where finding the log files/ the different categories of logging/ the different performance counter categories.			
SOW	[SOW-343]	The Contractor's Maintenance Manual SHALL provide the description for the usage of all third-party applications needed to configure, manage and maintain the system.			
SOW	[SOW-344]	The Contractor's Maintenance Manual SHALL provide the descriptions of all indicators, switches, switch positions, and displays.			
SOW	[SOW-345]	The Contractor's Maintenance Manual SHALL define the in-depth, step-by-step procedure how to perform the 1st, 2nd and 3rd level corrective and preventive maintenance tasks and SM&C tasks.			
SOW	[SOW-346]	The Contractor's Maintenance Manual SHALL include a maintenance plan to cover all the preventive maintenance activities based on the operational time or calendar time as applicable.			
SOW	[SOW-347]	The Contractor SHALL ensure the Procedures contained in the manuals are an outcome of the O&M Task analysis requested in Section 11.5.2.			

SOW	[SOW-348]	The Contractor SHALL ensure the manual includes an annex with troubleshooting information that provides breakdowns of actions to be performed to solve a full range of (potential) problems or provide workarounds (Problem Management).			
SOW	[SOW-349]	The Contractor SHALL ensure the manual contains all possible configuration information and settings.			
SOW	[SOW-350]	In case Software Identifier (SWID) tags cannot be automatically installed by software installers (e.g., legacy or third party software), the Contractor SHALL include in installation documentation descriptions of the process to manually install SWID tags.			
SOW	[SOW-351]	The Contractor SHALL ensure the manual contains all possible information on the use and locations of Log Files.			
SOW	[SOW-352]	The Contractor SHALL ensure that each and every procedure include as a minimum the following information: o The support level to be assigned; o Location/facility involved (if the operation is performed remotely, it has to be specified); o Personnel skills required; o Task duration and frequency (if applicable), reusing MTBF and MTTR data available; o Manpower required; o Tools, test equipment and special tools required (if any); o The steps needed to perform the procedure.			
SOW	[SOW-353]	The Contractor SHALL provide OEM manuals for all Commercial Off-the-Shelf (COTS) hardware and software installed.			
SOW	[SOW-354]	The Contractor SHALL be responsible to keep the COTS OEM manual under configuration control and to assure that all the COTS OEM Manuals will be always coherent with the operation configuration deployed, i.e., OBL.			
SOW	[SOW-355]	The Contractor SHALL assure that all the possible information needed to configure, operate, manage and maintain the COTS product will be in the User Manual and in the Maintenance Manual if they are no in the COTS OEM manuals.			
SOW	[SOW-356]	The Contractor SHALL provide as-built installation drawings, which reflect the complete installation conducted by the Contractor for each site.			
SOW	[SOW-357]	The as-built drawings SHALL comprise of: o Layout Plans showing the locations of all Contractor installed assets; o Cabling Plans showing all Contractor installed cabling, per security classification, clearly identifying the location and labelling of each cable, together with the terminations at both ends and the use of the cable; o Rack Layout Plans for all Contractor installed racks; o System Configuration Plan showing all installed assets with all their interfaces and interconnections, both internal and external.			
SOW	[SOW-358]	The Contractor SHALL ensure that all as-built drawings are cross-referenced and consistent with each other and with any other documents provided under this Contract, such as manuals and training material.			
SOW	[SOW-359]	As-build drawings representing technical networking and service configuration diagrams SHALL use layered views, as follows: o One layer SHALL be created for the physical view, covering hardware, ports and cable-connections (including also signal flow, electrical power and grounding); o One layer for the logical view, covering VLANs, virtual servers, logical links; o One layer for the addressing and routing information; o Service view schematics.			
SOW	[SOW-360]	The Contractor SHALL ensure all Other Project Documentation respects the general requirement about publications in this SOW (SOW 11.6.12; SOW 11.6.13 as a minimum).			
SOW	[SOW-361]	The Contractor SHALL prepare and submit for approval a set of business rules which explain the harmonization criteria of all the technical documentation in terms of fonts, numbering, bullet points and all the publication rules to be used for the complete set of documentation. The business rules will be applicable for both Paper and electronic publication.			
SOW	[SOW-362]	The Contractor SHALL ensure all Manuals are printable if required and therefore the page format SHALL be A4, printable in loose-leaf form, and possible to be presented bound in stiff backed covers with 4-ringed binders which permit the removal and insertion of individual pages and drawings.			
SOW	[SOW-363]	The Contractor SHALL ensure each page contains the appropriate NATO classification of the manual at the top and bottom of each page.			

SOW	[SOW-364]	The Contractor SHALL ensure all pages containing drawings and schematic diagrams are of the same size as other pages of the manuals.			
SOW	[SOW-365]	The Contractor SHALL place the appropriate security classification in the identification block of each drawing.			
SOW	[SOW-366]	The Contractor SHALL deliver soft copies of any composed or compiled documentation in Compact Disc Read-Only Memory (CD-ROM) or digital versatile disc (DVD) format.			
SOW	[SOW-367]	The Contractor SHALL ensure all documentation delivered in this Contract is compatible with Microsoft Office Professional and Adobe PDF.			
SOW	[SOW-368]	The Contractor SHALL deliver O&M Manuals in Microsoft Office Professional or PDF format, if available. If not available in this format, another common format may be accepted. If the commercial documentation is not available in CD-ROM, another form of electronic media is acceptable with the prior authorization of the Purchaser PM.			
SOW	[SOW-369]	The Contractor SHALL ensure the physical support of electronic, optical or soft copies of documents display the highest level of the classification of their contents.			
SOW	[SOW-370]	The Contractor SHALL ensure the Header and/or Title of the directory structure of documentation provided in soft copy format bears a reminder of the highest classification level of its contents.			
SOW	[SOW-371]	For ease of handling, the Contractor SHALL separate unclassified from classified documentation and provided it on separate CD-ROMs or DVDs.			
SOW	[SOW-372]	The Contractor SHALL be the responsible authority for the issue, control, and distribution of amendments to delivered documentation in the format provided for the associated equipment or system until expiration of the warranty period.			
SOW	[SOW-373]	The Contractor SHALL test and validate the procedures and resources described in the technical manuals.			
SOW	[SOW-374]	The Contractor SHALL provide all the technical documentation at least 12 weeks prior to the final delivery dates outlined in SSS to enable the Purchaser to perform a detailed review as the content matures and leave sufficient time for the updates resulted by the review. The Contractor SHALL include the documentation release plan within the first version of ILSP for approval, to provide Purchaser enough visibility for the schedule.			
SOW	[SOW-375]	Not later than one (1) month prior to the delivery of the IEG-C at the first location, the Contractor SHALL submit a copy of the final technical and training publications to the Purchaser for review.			
SOW	[SOW-376]	Any resulting recommended changes, corrections and/or additions submitted by the Purchaser SHALL be incorporated by the Contractor in the final version.			
SOW	[SOW-377]	The Contractor SHALL provide the final versions of each Technical Publication, and Training Material in the requisite number of copies within four (4) weeks of FSA.			
SOW	[SOW-378]	Until the expiration of the warranty, the Contractor SHALL remain responsible for any changes to the manuals and training material required as a result of any omission or inaccuracy discovered in use or, whenever changes/modifications in equipment or spare parts are made under the Contractor's responsibility.			
SOW	[SOW-379]	The Contractor SHALL deliver two copies on CD-ROM of the IEG-C Operations Manuals for each of the sites, plus two copies for the NCI Agency.			
SOW	[SOW-380]	In addition to the “Manual Issuing schedule”, the Contractor SHALL update all Manuals as needed throughout this contract.			
SOW	[SOW-381]	The Contractor SHALL provide all training modules and courses required to enable all initially assigned the Purchaser personnel to operate and maintain the system at Level 1, 2 and 3. The Contractor SHALL ensure all activities, milestones and actors associated with IEG-C System Training are guided by the Training Plan.			
SOW	[SOW-382]	The Contractor SHALL design, develop and deliver minimum the following trainings: o System operations training o System maintenance training o Guard administration training o Other administration trainings (e.g. SMC, Security) identified during TNA o Train the Trainer (TtT) trainings o Test Crew trainings o Transition Training (in each site).			

SOW	[SOW-383]	The Contractor SHALL design, develop, deliver and maintain the following types of training: o Classroom Training (for operators, system administrators, guard administrators, engineers) o On the Job Training (for operators, system administrators, guard administrators, engineers) o Computer Based Training (CBT) modules for self-paced individual learning, compatible with the NCIA Learning Management System (only for NU).			
SOW	[SOW-384]	As part of the system implementation the Contractor SHALL provide on-site training to all support staff designated by the Site POC and on all tasks required to operate, maintain and recover the IEG-C System.			
SOW	[SOW-385]	As part of the training process the Contractor SHALL provide the on-site training course (operators, administrators/maintainers and trainers) for a maximum number of two sessions in Mons for each type of training as outlined in [SOW-384], or another site designated by the Purchaser or an online course. The Contractor SHALL provide the Site Transition Training in each installation site both for operation and Level 1 maintenance, as applicable.			
SOW	[SOW-386]	The Contractor SHALL provide each training session for a maximum of 12 persons per session.			
SOW	[SOW-387]	The Contractor SHALL use the Training Needs Analysis (TNA) to refine the number of training sessions needed for each role.			
SOW	[SOW-388]	The Contractor SHALL deliver any additional training sessions that may be deemed necessary after completion of TNA at no additional cost to the Purchaser.			
SOW	[SOW-389]	As part of the training process the Contractor SHALL provide Train the Trainer courses for a minimum of 5 instructors designated by the Purchaser.			
SOW	[SOW-390]	Training and all related training documentation SHALL be provided in the English language.			
SOW	[SOW-391]	Training Courses SHALL be completed before the PSA (EDC+20mo) milestone, with the exception of the Test Crew trainings which SHALL be provided before the official test events start.			
SOW	[SOW-392]	The Contractor SHALL provide all other facilities, services and equipment (including servers and workstations for students and teachers, network equipment, all required software, etc.) necessary to carry out the On-Site Training activities.			
SOW	[SOW-393]	The Contractor SHALL identify the eventual prerequisite of the personnel for training participation as part of the TNA.			
SOW	[SOW-394]	The Contractor SHALL train the Reference and Testing Facility staff to operate the Reference and Testing Facility, through attending a short, informal, on-site training course that the Contractor SHALL prepare, organise and lead.			
SOW	[SOW-395]	The Contractor SHALL provide training for all releases of the project.			
SOW	[SOW-396]	The Contractor SHALL ensure the Training Materials include how the Transition from one Release to the next release is realised and how to install, configure and maintain the Modified or new Component capability, including COTS components.			
SOW	[SOW-397]	If activated, the Contractor SHALL provide all training related services and deliverables in accordance with Section 6.6 for each optional site and service outlined in the SSS.			
SOW	[SOW-398]	The Contractor SHALL base the Training Process and Procedures on the results of the Contractor's TNA.			
SOW	[SOW-399]	The Contractor SHALL detail its approach and planning on how the TNA process will be performed and managed within its Training Plan.			
SOW	[SOW-400]	The Contractor SHALL conduct a TNA in accordance with the [BiSC D-075-007, 2015]. The TNA SHALL include (as a minimum): o A Target Audience Analysis o A Performance Gap Analysis o A Difficulty, Importance and Frequency (DIF) Analysis; o A Training Delivery Options Analysis			
SOW	[SOW-401]	The Contractor SHALL base the TNA on the tasks resulting from Task Analysis carried out as part of the LSA Process and on the possible gaps highlighted during the site surveys (so called Target Audience Analysis).			
SOW	[SOW-402]	The Contractor SHALL ensure the TNA considers all staff roles involved in IEG-C System operation, administration, maintenance and support at all levels as they are assigned within Purchaser organization. For this purpose, the Contractor SHALL use the roles identified under training requirements as baseline and finalize the list of the roles as part of TNA and based on Purchaser input.			
SOW	[SOW-403]	The Contractor SHALL perform the TNA and create the courses as applicable for different types of administrators, operators, maintenance, and support personnel as they are assigned within Purchaser organization.			
SOW	[SOW-404]	The Contractor SHALL deliver a TNA Report that captures the results of the TNA for Purchaser approval. The TNA report SHALL include the following:			

SOW	[SOW-405]	The Contractor SHALL develop and provide an IEG-C System Training Plan. The Training Plan SHALL be updated to address the results of the TNA.			
SOW	[SOW-406]	The Contractor SHALL develop and provide a Training Plan that describes how it will meet the Training requirements outlined in the contract and found after the TNA for initial and follow-on training.			
SOW	[SOW-407]	The Contractor SHALL develop and provide a Training Plan that describes the quality management process for training.			
SOW	[SOW-408]	The Contractor SHALL develop and provide a Training Plan that addresses all stages of training development, delivery, and support covered under this Contract.			
SOW	[SOW-409]	The Contractor SHALL develop and provide a Training Plan that describes in a coherent way how training will be designed, developed, delivered, and maintained throughout the life of the IEG-C System.			
SOW	[SOW-410]	The Contractor SHALL develop and provide a Training Plan that includes training design documentation using the Course Control Document III – Programme of Classes template provided in [BiSC D-075-007, 2015] Annex R-4.			
SOW	[SOW-411]	The Contractor's Training Plan SHALL take the TNA results into consideration, and based on the TNA results it SHALL propose the specific courses for all maintenance levels and operation.			
SOW	[SOW-412]	The Contractor's Training Plan SHALL propose the different training types (classroom, on the job training, train the trainer and CBTs) for each course for Purchaser approval.			
SOW	[SOW-413]	The Contractor SHALL describe in this plan the approach to training, milestones, organization and resource requirements, management structure, interrelationships and other tasks related for training development.			
SOW	[SOW-414]	The Contractor SHALL develop and provide a Training Plan that describes the training documentation for each course including but not limited to the syllabuses, schedules, course prerequisites (both for attendees and physical resources), course descriptions and training materials, method of evaluations and instructors.			
SOW	[SOW-415]	The Contractor SHALL recommend in this plan the mode(s) of training (e.g., formal classroom, individual computer-based, on-the-job, commercial or a combination) and the rationale for these recommendations for each type of training (User , Administrator, etc.).			
SOW	[SOW-416]	The Contractor SHALL develop and provide a Training Plan that describes the transition training process.			
SOW	[SOW-417]	The Contractor SHALL develop and provide a Training Plan that describes the support to be provided by the Purchaser (manpower, services, and material).			
SOW	[SOW-418]	The Contractor's Training Plan SHALL describe the basic physical classroom and infrastructure required to perform the training in Purchaser locations.			
SOW	[SOW-419]	The Contractor SHALL prepare all e-learning training material in compliance with the Sharable Content Object Reference Model (SCORM) edition 2004.			
SOW	[SOW-420]	The Contractor SHALL produce CBT/E-Learning material that complements the IEG-C classroom training by defining and explaining key concepts and terminology of the operational processes as incorporated into IEG-C features and functions.			
SOW	[SOW-421]	The Contractor SHALL produce a CBT/E-Learning Package that allows modifications by the Purchaser to reflect changes in the training concept and/or content without any additional cost to NATO.			
SOW	[SOW-422]	The Contractor SHALL produce a CBT/E-Learning Package to provide the system administrators with a generic view of the system functionalities, operational aspects, troubleshooting and maintenance.			
SOW	[SOW-423]	The Contractor SHALL provide all the appropriate training documentation to support the Purchaser Personnel to test, operate and maintain the IEG-C System and its support equipment.			
SOW	[SOW-424]	Each training course material SHALL be provided for Purchaser review minimum 8 weeks before the start of the training courses.			

SOW	[SOW-425]	The Contractor SHALL generate the following Training Material: o Training syllabus, o Student manual o Instructor guide and material o Learning guide o Quick reference card o Upon completion, a training certificate o Course evaluation feedback form o Performance support materials to support users after the training during their work, with the following characteristics: 'bite-sized' learning chunks (maximum 5 minutes of learning time), designed to model or explain concrete tasks.			
SOW	[SOW-426]	The Contractor SHALL ensure the Training documentation conforms to the standards outlined in the training Section of the SOW and SRS.			
SOW	[SOW-427]	The Contractor SHALL ensure the Training documentation (Including the E-Learning Material) is developed in accordance with the results of the TNA.			
SOW	[SOW-428]	The Contractor SHALL ensure the training materials for the IEG-C System-specific courses provide all the information required to conduct the courses and maintain the training materials.			
SOW	[SOW-429]	The Contractor SHALL ensure the materials follow an existing instructional methodology that links training objectives with course structure, instructional techniques, course content, and assessment tools.			
SOW	[SOW-430]	For the development of training material, the Contractor SHALL reuse existing COTS documentation and manuals to the maximum extent possible.			
SOW	[SOW-431]	The Contractor SHALL ensure all course content is referenced to commercial or Contractor-developed documentation -- preferably user or technical manuals -- that describe the subject matter and are available on-site to students after course completion.			
SOW	[SOW-432]	The Contractor SHALL ensure the hands-on exercises included in the Training Process incorporate all IEG-C System implementation activities at a site.			
SOW	[SOW-433]	The Contractor SHALL ensure that the IEG-C System Training Materials are all provided in the UK English language. It may be assumed that all Purchasers personnel selected to attend the courses will meet the minimum Standardised Language Proficiency (SLP) of 3232 in English as specified in [STANAG 6001, 2014].			
SOW	[SOW-434]	The Contractor SHALL include, in the Training presentation materials, all slides or other information to be presented by the instructor during the course.			
SOW	[SOW-435]	The Contractor SHALL include, a Training Syllabus containing the following elements: o Course title, o Course description, o Learning objectives, as identified in the TNA and confirmed in the Training Plan, o Entry profile, o Concepts, Functions and Features presented in the course, o Instructional methodologies to be employed in the delivery of the course, o In-class assignments or laboratories, o Evaluation tools, o Performance standards.			
SOW	[SOW-436]	The Contractor SHALL develop and provide a Student Handbook for each course.			
SOW	[SOW-437]	The Contractor SHALL develop and provide a Student Handbook that provides the student with necessary information on all lesson objectives and contents, guidance for all learning activities and cross-references to assist the students in achieving the course objectives.			
SOW	[SOW-438]	The Contractor SHALL ensure that the Student Manuals take into account results from the DIF analysis and SHALL enable students to perform their major tasks.			
SOW	[SOW-439]	The Contractor SHALL ensure the System Operations training provides all necessary information, description and operational tasks to enable the Purchaser operators to use and perform the Level 1 maintenance activities.			

SOW	[SOW-440]	The Contractor SHALL ensure the Test Crew training provides all necessary information for the system specifications, testing environment, tools and test procedures for Purchaser test crew to be able to support the test activities. This training SHALL not exceed 4 hours in total with maximum of 12 participants.			
SOW	[SOW-441]	The Contractor SHALL ensure the Transition Training provides all necessary information for on-site (i.e. local maintenance and support personnel) Purchaser personnel to understand the system and its components, installation, connections and wirings, system components, preventive maintenance tasks, system shut-down and restart, disaster recovery, corrective maintenance tasks (e.g. troubleshooting, removal/replacement, software installation), and configuration system back-up procedures,. This training SHALL aim to enable the on-site transition to operations for each site, and therefore it may have certain commonalities with the 'Systems Operations' and 'System Administration and Maintenance' training.			
SOW	[SOW-442]	The Contractor SHALL ensure the System Administration and Maintenance Training provides as a minimum the following training on the capability (up to Level 2 and Level 3): o How to install, configure and maintain the capability, including COTS components. o How to maintain the Capability and how to use the logging and performance counters provided by the Capability. It includes as a minimum: o All the configuration settings for the Capability modules, services and components o How to configure the logging and uses of performance counters o Where to find the log files o The different categories of logging o The different performance counter categories o SMC procedures o How to troubleshoot the system, including actions to solve a full range of (potential) problems or provide workarounds. o How to manage database information, including database tables, triggers and stored procedures. o How perform back-up and restore procedures. o How to maintain the CMDB,			
SOW	[SOW-443]	The Contractor SHALL provide an Instructor's Guide for each training course. It SHALL contain all necessary information to prepare and conduct lessons and to evaluate students, including exercises, quizzes, and examinations and their corresponding answer sheets.			
SOW	[SOW-444]	The Contractor SHALL ensure the training materials also provide notes to instructors to assist in conducting the lecture or exercise. The Contractor SHALL provide the Presentation materials in Microsoft PowerPoint.			
SOW	[SOW-445]	The Contractor SHALL ensure the IEG-C capability Instructor Guide details the sequence of course instruction, providing references to the applicable training presentation materials, assignments and laboratories, evaluation tools and answer keys, Student Manual, and the Capability on-line help function. Within the Instructor Guide, the Contractor SHALL also include: o Materials for in-class assignments and laboratories. o Sample evaluation tools and answer keys. o Training System installation and configuration procedures. o The Contractor SHALL create and submit a summary of the recommended Training Materials, aids and equipment.			
SOW	[SOW-446]	The Contractor SHALL propose an assessment and evaluation methodology to the Purchaser as part of the Training Plan.			
SOW	[SOW-447]	The Contractor SHALL base the Training Assessment methodology on Sections 7-6 and 7-7 of [BiSC D-075-007, 2015] for assessment approaches and instruments and include as a minimum: o Examination methodologies and certification o Minimum score to achieve for successfully passing the course o Course(s) to be done to get the certification for each role o Description of Role's certification process.			
SOW	[SOW-448]	The Contractor SHALL ensure that each student is instructed at the end of each course or use of a Computer Based Training (CBT) to complete and return the course evaluation feedback form provided as part of the training course or E-Learning product.			

SOW	[SOW-449]	The Contractor SHALL consolidate and forward student feedback to the Purchaser following each training course in the form of a Training Evaluation Report. The report SHALL also recommend changes and improvements to the training plan based on the consolidated student feedback.			
SOW	[SOW-450]	In the report, the Contractor SHALL also address student attendance, problems encountered and actions taken to resolve the problems.			
SOW	[SOW-451]	The Contractor SHALL revise/refine and reissue course material and CBT products to reflect the consolidated student feedback and proposed improvements in the training evaluation report.			
SOW	[SOW-452]	The Contractor SHALL produce Training Certificates for each training session and student.			
SOW	[SOW-453]	The Contractor SHALL deliver Training Certificates later than two weeks following the completion of training.			
SOW	[SOW-454]	The Contractor SHALL provide the Purchaser's ILS POC with a System Inventory in electronic Microsoft Excel format at least 15 (fifteen) working days before the first delivery of equipment.			
SOW	[SOW-455]	The System Inventory is site-specific and SHALL include all items furnished under this Contract, as follows: o All main equipment – i.e. all CIS items, both COTS and Developed, down to replaceable item level, hierarchically listed conform configuration item decomposition, including groups and assemblies; all installed hardware, such as equipment racks; all LRU interconnecting equipment when they are special-to-type (e.g. special-to-type cables); o All ancillary equipment – i.e. all secondary items not essential to the functioning of the system, but deemed essential to the operation of the system, such as an all-weather canopy or a tool box; o All support equipment – i.e. all tools, test equipment and PHS&T equipment; o All Purchaser Furnished Equipment (PFE); o All Purchaser and Contractor provided software; o All spare parts, to include all spares, repair parts, and consumables, separated into technical and non-technical consumables; o All documentation, such as manuals, handbooks and drawings; and o All training materials.			
SOW	[SOW-456]	The Contractor SHALL use the inventory template provided the Purchaser to develop and submit the System Inventory. This template will be provided by the Purchaser after Contract Award.			
SOW	[SOW-457]	The Contractor SHALL provide the tempest specific part information additionally in the Inventory List for the tempested items.			
SOW	[SOW-458]	The depth and content of the Inventory List SHALL be subject to the Purchaser Approval.			
SOW	[SOW-459]	On the basis that an adequate manufacturer's identification numbering system is in place, NATO codification (the request and assignment of NATO Stock Codes – NSN) are not be required. In all other cases, NATO codification SHALL be required and the Contractor SHALL support the NATO codification process in accordance with the requirements of AcodP-1 and the requirements of the STANAGs referenced and included in AcodP-1, i.e. STANAG 3150, STANAG 3151, STANAG 4177, STANAG 4199 and STANAG 4438.			
SOW	[SOW-460]	All equipment SHALL be labelled in compliance with the Purchaser regulation and guidance. Labels SHALL at least contain the Contractor/OEM's name, identification, part number and serial number to ensure proper and quick identification of equipment down to the LRU level.			
SOW	[SOW-461]	The Contractor SHALL provide the details of the labelling approach in the CM Plan for Purchaser approval. The Contractor SHALL provide its labelling for the items that are configured and/or modified after procurement from the OEM. For these items, the Contractor SHALL assign a P/N for that specific configuration. The format and content of the labelling SHALL be provided to the Purchaser for			
SOW	[SOW-462]	Labelling SHALL be accomplished in a manner that will not adversely affect the life and utility of the assembly or module. Whenever practicable, the label SHALL be located in such a manner as to allow it to be visible after installation.			
SOW	[SOW-463]	Marking SHALL be as permanent as the normal life expectancy of the material on which it is applied and SHALL be such as required for ready legibility and identification.			
SOW	[SOW-464]	Marking SHALL be capable of withstanding the same environment tests required of the part and any other tests specified for the label itself. When possible, letters, numerals, and other characters SHALL be of such a size as to be clearly legible.			
SOW	[SOW-465]	All labelling and marking SHALL be in English language.			

SOW	[SOW-466]	Nameplates SHALL be attached to all major units of the system. Nameplates SHALL be in the English language with non-erasable letters/ numbers, clearly identifying the unit (unit designator); location code; as well as the Contractor or OEM CAGE code, part number and serial number. These plates SHALL be properly attached in a prominent position on each major unit to enable reading and control with easy access when installed. For the items requiring special handling and/or lifting up with additional tools due to heavy weight or high volume (dimensions), special plates including the weight, dimensions and lifting points information SHALL be provided on the items. Also these items SHALL have the adequate provisioning points to enable such special handling and lifting conditions.			
SOW	[SOW-467]	All equipment labels delivered by the Contractor SHALL contain a machine-readable code (e.g. barcode) compliant with ~~[STANAG 4329] and [AAP-44(A)]~~ AITP-09 and in accordance with the NATO coding scheme, which will be provided by the Purchaser at the request of the Contractor. In case NATO asset labels are provided by the Purchaser, the Contractor SHALL apply those labels in addition to the Contractor's labelling.			
SOW	[SOW-468]	The Contractor SHALL utilize these machine readable codes during the project to ensure that the following activities are carried out as efficiently as possible: o inventory checking; o codification, when required; o configuration auditing; o equipment PHS&T; o equipment delivery, placement and acceptance; o Maintenance.			
SOW	[SOW-469]	The Contractor SHALL provide a single, fully detailed, site-specific and priced Recommended Spare parts List (RSPL) that SHALL detail comprehensively all spare parts, tools, test equipment, and consumables required to operate and maintain the system at all levels of support, and in accordance with the RAMT requirements specified in the Contract, no later than 8 weeks before PSA (EDC+20mo) meeting.			
SOW	[SOW-470]	The RSPL SHALL separately list L1/2/3 (LRUs) items and L4 items (SRUs).			
SOW	[SOW-471]	The RSPL will be used by the Purchaser to evaluate the support concept and initial provisioning of Contractor-provided spares.			
SOW	[SOW-472]	The RSPL SHALL include, the following items: o Spare LRUs; o Spare special-to-type LRU interconnecting equipment; o Spare ancillaries; o Support equipment, such as tools, test equipment and PHS&T equipment; o Repair parts; o Technical and non-technical consumables.			
SOW	[SOW-473]	The RSPL SHALL include the following data elements: o Nomenclature; o Contractor/OEM CAGE code, part number and serial number; o Mean Time Between Failures (MTBF) – when applicable; o Indication Repairable (ND) or Non-Repairable (XB); o Turn Around Time (when repairable), lead time (new items); o Population, by system, site and total; o Recommended quantity; o Indication SPOF or part of a redundant array; o Unit price (including warranty and PHS&T) and minimum order quantity; o Unit repair cost (for repairable items; including warranty and PHS&T);			
SOW	[SOW-474]	The Contractor SHALL provide a set of spares calculated with 98% confidence level (site level) and assumption of continuous operation for a year.			
SOW	[SOW-475]	The Contractor SHALL provide the spare part calculations as a part of the Support Case.			

SOW	[SOW-476]	The Contractor SHALL also provide the technical consumables (filters, batteries, etc.) for preventive maintenance that will be enough for approximately a year after FSA. The shelf life of these consumables SHALL be long enough to be usable until the end of first year from FSA.			
SOW	[SOW-477]	The Contractor SHALL deliver the set of the spares and consumables before PSA (EDC+20mo).			
SOW	[SOW-478]	The Contractor SHALL provide all tools and test equipment required to perform L1/2/3 maintenance, as identified in the RSPL.			
SOW	[SOW-479]	Procurement and replenishment of L1/2/3 spare parts, including PHS&T, SHALL be the responsibility of the Contractor as per the Contract until FSA. Procurement, provisioning and replenishment of technical and non-technical consumables SHALL also be the responsibility of the Contractor.			
SOW	[SOW-480]	The Contractor SHALL provide a detailed Software Distribution List (SWDL), which SHALL detail comprehensively all Computer Software Configuration Items (CSCI) and associated software, firmware or feature/performance licenses provided under this Contract. The SWDL SHALL include, the following data elements: 1) CSCI identification number; 2) nomenclature; 3) version number; 4) license key (if applicable); 5) license renewal date (if applicable); 6) warranty expiration date; 7) date of distribution; 8) distribution location (geographically); 9) distribution target (server); and 10) Owner.			
SOW	[SOW-481]	The Contractor SHALL make sure that all licenses are originally registered with the Purchaser as end-user.			
SOW	[SOW-482]	The Contractor SHALL, for the purpose of transportation, package, crate, or otherwise prepare items in accordance with the best commercial practices for the types of supplies involved, giving due consideration to shipping and other hazards associated with the transportation of consignments overseas.			
SOW	[SOW-483]	Any special packaging materials required for the shipment of items SHALL be provided by the Contractor at no extra cost to the Purchaser.			
SOW	[SOW-484]	The packages, palettes and/or containers in which supplies are transported SHALL, in addition to normal mercantile marking, show on a separate nameplate the name of this project, contract number and shipping address.			
SOW	[SOW-485]	In the case of dangerous goods and goods requiring export licenses, the Contractor SHALL ensure that all required forms and certificates are provided and that all regulations for such goods are followed.			
SOW	[SOW-486]	For the purpose of transportation, all supplies SHALL be packaged to withstand the shipping hazards applicable to the chosen mode of transportation. Any special packaging materials required SHALL be provided by the Contractor and disposed of by the Contractor after unpacking, insofar as the packaging is not retained with the system (e.g. for storage of spares or return of failed equipment).			
SOW	[SOW-487]	The Contractor SHALL provide a confirmation of delivery to the Purchaser’s ILS POC within two weeks after each shipment. This confirmation SHALL summarize the supplies delivered, state the date of delivery, and provide a scan of the signature of the Purchaser POC on-site, receiving the supplies.			
SOW	[SOW-488]	The Contractor SHALL be responsible of removal and disposal of all packaging material after installation in each site.			

SOW	[SOW-489]	The Contractor SHALL produce and provide packing lists that accompany each shipment, which will include the following: o The Purchaser's contract number o The NATO project number o Names and addresses of the Contractor and the Purchaser; o Names and addresses of the Carrier, Consignor and Consignee (if different from Contractor or Purchaser) o Final destination address and POC; o Method of shipment o For each item shipped: Contract Line Item Number (CLIN) number as per the SSS; nomenclature; part number; serial number; and quantity o For each box, pallet and container: box/pallet/container identification number and number of boxes/pallets/containers; weight; dimensions.			
SOW	[SOW-490]	The Contractor SHALL ensure that two copies of the packing lists are fastened in a weather-proof, sealed envelope on the outside of each box, palette and/ or container, and one packing list put inside each container/box.			
SOW	[SOW-491]	The Contractor SHALL be responsible for all handling and storage of equipment, packages, boxes and containers during the project.			
SOW	[SOW-492]	The Contractor SHALL also be responsible for organising and operating any handling equipment and storage facilities required.			
SOW	[SOW-493]	The Contractor SHALL arrange all that is necessary to access the sites where equipment is handled or stored.			
SOW	[SOW-494]	In the case of dangerous goods and goods requiring export licenses, the Contractor SHALL ensure that all required forms and certificates are provided and that all Host Nation regulations for such goods are followed. The Contractor SHALL provide a list of such equipment.			
SOW	[SOW-495]	The Contractor SHALL be responsible for transportation and delivery of all equipment furnished under this Contract from its site in a NATO nation to its respective implementation destination as outlined in Annex B1.			
SOW	[SOW-496]	Ten (10) working days before each shipment of supplies, the Contractor SHALL provide the Purchaser with a Notice of Shipment comprising the following details: o Shipment Date; o Purchaser Contract Number; o CLIN; o Consignor's and Consignee's name and address; o Number of Packages/Containers; o Gross weight; o Final/Partial Shipment; o Mode of Shipment (e.g., road…); o Number of 302 Forms used.			
SOW	[SOW-497]	The Contractor SHALL be responsible for any insurance covering these shipments.			
SOW	[SOW-498]	The Contractor SHALL also be responsible for transportation of repaired/ replacement items under warranty to the original location. Return of unserviceable equipment to Contractor facility for (warranty) repair/replacement is the responsibility of the Purchaser. However, if there are any special packaging requirements and materials required for the shipment, the Contractor SHALL be responsible providing the guidance and the special packaging material. Additionally, any export/import regulations and requirements SHALL be specified and directed by the Contractor.			
SOW	[SOW-499]	At the Purchaser designated staging area, the Contractor SHALL unload the equipment and move the equipment to its final destination for installation. The Contractor may use any support equipment provided by the Purchaser, but remains responsible for requesting, organizing and using any support equipment required to offload and move equipment to its final destination. If such support equipment is not available on-site, then the Contractor SHALL be the ultimate responsible to arrange such equipment with the shipment.			
SOW	[SOW-500]	The Contractor SHALL be responsible for customs clearance of all shipments into the destination countries. It is the Contractor's responsibility to take into account delays at customs. He SHALL therefore consider eventual delays and arrange for shipment in time. Under no circumstances can the Purchaser be held responsible for delays incurred, even when utilising Purchaser provided Customs Form 302.			

SOW	[SOW-501]	Prior to a shipment by the Contractor, the Purchaser will upon request issue a Customs form 302, which in some cases may facilitate the duty free import/export of goods. The Contractor SHALL be responsible for requesting the issue of a form 302 at least 10 (ten) working days prior to shipment. The request for a Form 302 SHALL be included with the Notice of Shipment and accompanied by one (1) additional packing list. The request is normally processed by the Purchaser within three (3) working days. The requested 302 forms will be sent by courier. The original 302 forms SHALL accompany the shipment and therefore no fax or electronic copy will be used, nor provided to the Contractor.			
SOW	[SOW-502]	If a country refuses to accept the Form 302 and requires the payment of customs duties, the Contractor SHALL pay these customs duties and the Purchaser SHALL reimburse the Contractor at actual cost against presentation of pertinent supporting documents. Should such an event occur, the Contractor SHALL immediately inform the Purchaser by the fastest means available and before paying, obtain from the Customs Officer a written statement establishing that his Country refuses to accept the Form 302.			
SOW	[SOW-503]	The Contractor SHALL be responsible for managing and performing all activities that is necessary to obtain export licenses for the goods requiring such licenses.			
SOW	[SOW-504]	The Contractor SHALL provide a detailed list of the equipment requiring export licenses. The Contractor SHALL provide the necessary procedures that needs to be applied for items to be relocated for repair or any other purposes.			
SOW	[SOW-505]	The Contractor SHALL perform all the maintenance and support activities (Level 2, 3, and Level 4) starting with activation of the Reference Environment until the successful completion of PSA (EDC+20mo) milestone.			
SOW	[SOW-506]	The following criteria SHALL be met to achieve FSA: o In case of a critical failure in Reference Environment effecting the continuity of the operation, the Contractor SHALL restore the system maximum within 1 business day. o In case of a non-critical failure not effecting the operation, the Contractor SHALL fix the failure within 3 business days.			
SOW	[SOW-507]	The Contractor SHALL apply the formal Change Management process for the fixes requiring the change of the approved baseline.			
SOW	[SOW-508]	Starting from PSA (EDC+20mo) and until FSA (EDC+27mo) when all the site acceptance activities are completed; the Contractor SHALL be responsible for the Level 2, Level 3 and Level 4 maintenance and support activities in each activated site within the scope of the Initial Operational Support.			
SOW	[SOW-509]	In case of a critical failure in the systems effecting the continuity of the operation, the Contractor SHALL restore the system maximum within 3 business days. In case of a non-critical failure not effecting the operation, the Contractor SHALL fix the failure within 10 business days.			
SOW	[SOW-510]	This support SHALL include, but not limited to, Level 2 maintenance that will focus on using Built-In Test Equipment (BITE), standard tools and test equipment, on-equipment, day-to-day corrective and preventive maintenance. This SHALL include replacement of LRU's, manual reconfiguration and adjustments, detailed baseline inspections and checkouts, fault identification and isolation, problem management, limited calibrations, and minor equipment repairs.			
SOW	[SOW-511]	This support SHALL include, but not limited to, the Level 3 maintenance and support will constitute the engineering level. It SHALL include in-depth testing, problem and modification analysis, release management, complex repairs and replacements, node and mission configuration(if applicable), calibration, scheduled servicing, overhaul and rebuild, implementation of major and/or critical changes, baseline restoration, post-maintenance review, supply support and PHS&T.			
SOW	[SOW-512]	This support SHALL include the Level 4 maintenance that involves standard warranty type services for repair or replacement of the items.			
SOW	[SOW-513]	If activated by the Purchaser, the Contractor SHALL extend the operational support period as options outlined in SSS.			
SOW	[SOW-514]	The Contractor SHALL warrant that all equipment and software furnished under this Contract and all installation work performed under this Contract conform to the requirements and is free of any defect in material, code or workmanship for a period starting at date of FSA to date of FSA plus one (1) year.			
SOW	[SOW-515]	The Contractor SHALL support the system as part of the project implementation scope from the first site activation until FSA (EDC+27mo) milestone is successfully completed. During this period, the Contractor SHALL provide on-site and off-site maintenance and support services as required.			
SOW	[SOW-516]	The Contractor SHALL fix/repair/replace all items received as per his internal procedures with the highest priority allocated. The Contractor SHALL provide the repaired/replacement item within maximum 20 business days after the Purchaser has provided the failure notification in written.			

SOW	[SOW-517]	The Contractor SHALL acknowledge and propose a corrective action for the failed components within two business days after the initiation of the warranty request. In the case of a failure could not be identified to an LRU level and/or could not be isolated within 3 business day (starting with the warranty request) even with on-call assistance from the Contractor, the Contractor SHALL dispatch a field engineer to provide a solution on-site.			
SOW	[SOW-518]	The Contractor SHALL provide a specific Customer POC for all warranty and support requests. The Contractor SHALL detail all the warranty and support requirements in its ISSP including the roles and responsibilities.			
SOW	[SOW-519]	The Contractor SHALL be responsible for the provision of any alternative or superseding items, should the original part be no longer available, ensuring compliance with the original design and System provided by this Contract. However, in such cases the Contractor SHALL propose the original alternative item for the Purchaser approval. The alternative item SHALL conform with all the specified quality requirements within the scope of the contract and standards.			
SOW	[SOW-520]	The Contractor SHALL provide a Technical Assistance to the Purchaser or his representatives during the warranty period. Technical assistance information details SHALL be indicated in the ISSP.			
SOW	[SOW-521]	The Technical Assistance SHALL provide on-call and/or on-site support in English for requests that correspond to information demands limited to the perimeter of delivered products, evolution proposals, problem reports, or any information needed by the Purchaser or its representatives, which are not included in the supplied technical documentation.			
SOW	[SOW-522]	If the Contractor becomes aware at any time before acceptance by the Purchaser that a defect exists in any supplies, the Contractor SHALL coordinate with the Purchaser and promptly correct the defect.			
SOW	[SOW-523]	Defect magnetic, solid state and electronic media storage devices (e.g., CD-ROM's, DVD's, Universal Serial Bus (USB) sticks, solid state storage drives, hard drives) SHALL remain NATO property, at no additional cost, and not be returned to the Contractor when being replaced.			
SOW	[SOW-524]	The Contractor SHALL replace any such defect storage devices with new storage devices at no additional cost to the Purchaser.			
SOW	[SOW-525]	The Contractor SHALL be responsible for the provision of any alternative or superseding items, should the original part be no longer available, ensuring compliance with the original design provided by this Contract.			
SOW	[SOW-526]	During the warranty period, the Contractor SHALL be responsible for supplying all COTS hardware and software upgrades and updates.			
SOW	[SOW-527]	The Contractor SHALL make the availability of COTS hardware and software upgrades and updates known to the Purchaser and, if proposed for introduction by the Contractor for whatever reason, including any corrective action for an identified fault, SHALL always be subject to Purchaser approval.			
SOW	[SOW-528]	The Contractor SHALL request formal authorization from the Purchaser to proceed with deactivation and removal of legacy equipment.			
SOW	[SOW-529]	The Contractor SHALL be responsible for the removal of the items from the installation facilities as required, and SHALL hand-over such devices to the Purchaser in local Purchaser warehouse.			
SOW	[SOW-530]	The Contractor SHALL work with local site personnel to ensure the controlled removal and disposal, unless otherwise specified by the Purchaser.			
SOW	[SOW-531]	The Contractor SHALL ensure the overall implementation at the sites respects the achievement of milestones as described in SECTION 3.			
SOW	[SOW-532]	The Contractor SHALL execute implementation activities in several steps:			
SOW	[SOW-533]	The Contractor SHALL conduct site surveys at all the sites related to the Site Activation and FSA milestones, and which are part of the contract (i.e., data centre sites, and additional options which have been activated under the contract; see SECTION 3). o The Contractor SHALL conduct complementary site surveys in addition to the ones conducted under pilot release – see 13.2 o The Contractor SHALL update and deliver the SIP – see 13.3 o The Contractor SHALL conduct site preparation activities – see 13.4 o The Contractor SHALL conduct site installation and activation activities – see 13.5.			
SOW	[SOW-534]	The Contractor SHALL follow the site survey process as described in SECTION 9: Site Surveys			
SOW	[SOW-535]	The Contractor SHALL adjust the activities and deliverables to the results of the site surveys.			
SOW	[SOW-536]	The Contractor SHALL propose, for Purchaser approval, the implementation sequence of sites implemented at PSA in the System Implementation Plan (SIP) (see ANNEX B).			
SOW	[SOW-537]	The Contractor SHALL produce and deliver a SIP that at least meet all contents requirements as laid out in section 15.11.			

SOW	[SOW-538]	The Contractor SHALL coordinate the installation and activation dates reflected in the SIP with the Purchaser and the Site POCs to accommodate site-specific requirements, exercises, holiday periods, and other considerations. Any such dates and any revision of these dates SHALL be coordinated with the Purchaser and the relevant sites at least four weeks before the start of the relevant activities.			
SOW	[SOW-539]	The Contractor SHALL provide each site POC, with a copy to the Purchaser Project Manager, with a draft list of hardware and software to be shipped, and a list of Contractor's personnel together with a copy of each person's Personnel Security Clearance (PSC) for those who will be involved in site installation and activation work.			
SOW	[SOW-540]	The Contractor SHALL monitor the progress of any required Site facilities preparations, and the progress of any required provision of input by the Purchaser and the Site, to ensure timeliness and quality of the preparatory work required from the Purchaser.			
SOW	[SOW-541]	The Contractor SHALL ensure that anything that may delay installation is brought to the attention of the Purchaser Project Manager promptly.			
SOW	[SOW-542]	The Contractor SHALL prepare and conduct a Site Verification Survey no later than two months prior to installation activities at the site. The purpose of this Site Verification Survey is to verify that the information provided by the site is still valid, and to perform any necessary updates to the system implementation documentation. The Contractor may recommend to the Purchaser that certain Site Verification Survey(s) are not warranted, which the Purchaser may accept or reject.			
SOW	[SOW-543]	The Contractor SHALL issue the updated SIP immediately after the Site Verification Survey and no later than two weeks before the Site installation.			
SOW	[SOW-544]	The Contractor SHALL produce a Site Activation/ Acceptance Plan in coordination with the Purchaser.			
SOW	[SOW-545]	The Contractor SHALL perform site installation and activation at any site, which comprises the following activities: o Perform site installation of any IEG-C elements (Hardware, Software), including establishment of network connectivity between all required components. o Perform site activation. o Execute all activities related to security accreditation. o Execute Physical Configuration Audit (PCA). o Deliver all documentation associated to site installation and activation.			
SOW	[SOW-546]	The Contractor SHALL coordinate the start date of the planned installation no later than three weeks before that start date.			
SOW	[SOW-547]	Throughout all Site installation activities the Contractor SHALL hold a daily meeting with the site POC to agree on the work to be conducted during the day.			
SOW	[SOW-548]	Although the Purchaser will provide the facilities in which the IEG-C will be installed and the external systems to which it will be interfaced, the Contractor SHALL be responsible for timely and complete delivery and installation of all relevant supplies.			
SOW	[SOW-549]	The Contractor SHALL ensure that the equipment to be installed in any of the relevant site facilities (as identified by the site during the site survey) has been tested and certified to operate at the "facility's zone level". The Contractor SHALL provide relevant evidence to the site before installing any IEG-C piece of equipment.			
SOW	[SOW-550]	The Contractor SHALL unpack all IEG-C equipment at the installation location and dispose of packing materials as directed by the Purchaser's Site POC.			
SOW	[SOW-551]	The Contractor SHALL install all equipment in accordance with the applicable document indicated in [NCIA AI TECH 06.03.01, 2015].			
SOW	[SOW-552]	The Contractor SHALL connect all equipment to electrical power and communications interfaces provided by the Purchaser.			
SOW	[SOW-553]	The Contractor SHALL turn on all equipment and configure hardware and software settings to match the PBL and site infrastructure configuration.			
SOW	[SOW-554]	The Contractor SHALL perform site activation activities locally at the site.			
SOW	[SOW-555]	The Contractor SHALL ensure that none of the site activation activities have any impact on the NATO Staff Users' desktop applications, except for some authorised potential and limited outages.			
SOW	[SOW-556]	The Contractor SHALL conduct the site activation tests.			
SOW	[SOW-557]	For that purpose, The Contractor SHALL provide a Site Activation Test Report for each site.			
SOW	[SOW-558]	The Contractor SHALL execute Site Activation tests on the operational sites that demonstrate that the equipment installed so far (i.e., both on the individual site and system-wide if other sites have already been installed) provides the Contractual functionality and performance level, including all interfaces with all internal and external system, including administration requirements, and is ready for operational use.			

SOW	[SOW-559]	The Contractor SHALL carry out the site activation tests for a maximum of one week at each site, exclusive of any preparation time.			
SOW	[SOW-560]	For each of the sites where a component of the IEG-C system is to be installed and local management to be activated, the Contractor SHALL modify the approved generic SecOPs (see 16.1.3.8) to meet the requirements of the local site.			
SOW	[SOW-561]	The Contractor SHALL deliver and present the localised version of the IEG-C SecOPs to the local SAA for approval.			
SOW	[SOW-562]	The Contractor SHALL take into account any comments from the reviewers and Local SAA and SHALL update the document as many times as necessary in order to gain Local SAA approval of the IEG-C localised SecOPs for the site.			
SOW	[SOW-563]	For each site where a component of the IEG-C system is to be installed, the Contractor SHALL provide inputs to the local SSCS to meet the requirements of the local site.			
SOW	[SOW-564]	The Contractor SHALL deliver and present the proposed modifications of the SSCS to the local SAA for approval.			
SOW	[SOW-565]	The Contractor SHALL take into account any comments from the reviewers and Local SAA and SHALL update the proposal as many times as necessary in order to gain Local SAA approval of the IEG-C localised SSCS for the site.			
SOW	[SOW-566]	The Contractor SHALL support the local security staff in the completion of the SSCS.			
SOW	[SOW-567]	For each of the sites where a component of the IEG-C system is to be installed, the Contractor SHALL modify the approved generic STVP to meet the requirements of the local site.			
SOW	[SOW-568]	The Contractor SHALL deliver and present the localised version of the STVP to the local SAA for approval.			
SOW	[SOW-569]	The Contractor SHALL take into account any comments from the reviewers and Local SAA and SHALL update the document as many times as necessary in order to gain Local SAA approval of the IEG-C localised STVP for the site.			
SOW	[SOW-570]	The Contractor SHALL support the NCI Agency in the execution of the STVP.			
SOW	[SOW-571]	The Contractor SHALL schedule and perform the PCA with the Purchaser ILS POC.			
SOW	[SOW-572]	The Contractor SHALL co-ordinate the PCA with the Purchaser's ILS POC.			
SOW	[SOW-573]	The Contractor SHALL produce and deliver a PCA Report.			
SOW	[SOW-574]	The Contractor SHALL perform the corrective actions as outlined in the PCA Report.			
SOW	[SOW-575]	The Contractor SHALL deliver to the sites all documentation that is required for system implementation and operation.			
SOW	[SOW-576]	The Contractor SHALL update the documentation delivered at the sites to accommodate any site-specific changes and/or configurations.			
SOW	[SOW-577]	Upon completion of site implementation work, the Contractor SHALL provide the Purchaser with a copy of the site installation and activation checklist and resolve any discrepancies identified.			
SOW	[SOW-578]	The Contractor SHALL keep the Documentation under configuration control, as per section 18.11.			
SOW	[SOW-579]	All information items used during the verification and validation activities are to be classified and handled according to their security classification. Guidance is provided in this SOW, under the security section.			
SOW	[SOW-580]	The Contractor SHALL have the overall responsibility for meeting the TVV requirements and conducting all related activities. This includes the development of all TVV documentation required under this Contract, the conduct of all independent verification, validation and assurance events, and the evaluation and documentation of the results.			
SOW	[SOW-581]	All deliverables supplied by the Contractor under this contract SHALL be verified and validated to meet the requirements of this contract. All document-based deliverables SHALL be produced in a manner compliant with the templates provided by the Purchaser. In particular: o The Contractor SHALL perform the verification activities within each Build Process; o The Contractor SHALL perform verification to confirm that each element properly reflects the specified requirements, design, code, integration and documentation; o The Contractor SHALL support Purchaser led Validation Activities to confirm that the solution is fit for purpose.			
SOW	[SOW-582]	The Contractor SHALL be responsible for the planning, execution and follow-up of all TVV events. The Purchaser will assist in preparations by reviewing and providing feedback on all Contractor produced configuration items. The Purchaser will also provide testing and engineering Subject Matter Expertise (SME) during all TVV events to witness and assist with these events.			
SOW	[SOW-583]	The Contractor SHALL demonstrate to the Purchaser that there is a testing process in place for the project, supported by Contractor Quality Assurance (QA).			
SOW	[SOW-584]	Where requested by the Purchaser, the Contractor SHALL provide test data to support all TVV activities.			

SOW	[SOW-585]	The Contractor SHALL strictly follow the TVV processes (described in the latest version of the TV&V Process Definition and Execution Document (PDED) provided by the purchaser). When Contractor would like to propose a modification, it SHALL be approved by the Purchaser.			
SOW	[SOW-586]	The Contractor SHALL ensure that rigorous testing, including regression testing when required, is performed at every stage of the Project lifecycle in order to identify and correct defects as early as possible and minimise impact on cost and schedule.			
SOW	[SOW-587]	All test, verification and validation material developed and used under this contract SHALL be delivered to the Purchaser.			
SOW	[SOW-588]	The Contractor SHALL provide an overall project Test Director for the phases defined in Table 14: List of TVV Phases, who will work closely with the Purchaser's assigned TVV Manager and NATO Quality Assurance Representative (NQAR). Table 14: defines the test phases considered. If deemed necessary, IEG-C project may split the test phases defined in Table 14: into multiple events.			
SOW	[SOW-589]	The Contractor SHALL use Key Performance Indicators (KPIs) to identify opportunities for quality improvement, provide solutions and update the plans, the achievement of defined objectives like coverage of risks, requirements, supported configurations, supported operational scenarios, etc.			
SOW	[SOW-590]	The Contractor SHALL have the overall responsibility for meeting the TVV requirements and conducting all related activities defined in Table. Each phase may have one or more events to complete the full scope.			
SOW	[SOW-591]	The Contractor SHALL only proceed to the next formal TVV activity, after the successful completion of the previous TVV activity and after the agreement/approval by the Purchaser.			
SOW	[SOW-592]	The Contractor SHALL provide a System Test Documentation Package, following documentation templates provided by the Purchaser, that is comprised of the following documents in Table 15: Test Documentation:			
SOW	[SOW-593]	If applicable, the Contractor SHALL develop and validate any Test Harnesses, simulators and stubs, including all script/code/data/tools required to execute the planned functional and non-functional tests in the Test Environment. The Test Harnesses for PFE will be provided by the Purchaser.			
SOW	[SOW-594]	Modification of inaccurate or inadequate TVV deliverables and any subsequent work arising as a result SHALL be carried out at the Contractor's expense.			
SOW	[SOW-595]	All TVV materials developed and used under this contract SHALL be delivered to the Purchaser.			
SOW	[SOW-596]	Templates provided by the Purchaser are to be utilized by the Contractor as structure guides and for the content the Purchaser expects to be detailed. If the Contractor would like to propose a modification of the templates, it SHALL be approved by the Purchaser.			
SOW	[SOW-597]	All deliverables SHALL undergo as many review cycles are required, and SHALL be approved once all deficiencies have been corrected.			
SOW	[SOW-598]	The Contractor SHALL identify and describe in the Master Test Plan (MTP) which best practices and international standards will be applied and how.			
SOW	[SOW-599]	The Contractor SHALL produce a Master Test Plan (MTP) to address the plans for each TVV activities listed in this document. The Purchaser will monitor and inspect the Contractor's MTP activities to ensure compliance.			
SOW	[SOW-600]	The Contractor SHALL keep the MTP always up to date.			
SOW	[SOW-601]	The Contractor SHALL describe how the Quality Based Testing is addressed and implemented in the MTP. Figure 5: Product Quality Criteria is based on ISO 25010 and should be used as product quality criteria model.			
SOW	[SOW-602]	The Contractor SHALL describe all formal TVV activities in the MTP with a testing methodology and strategy that fit the development methodology chosen by the project.			
SOW	[SOW-603]	The Contractor proposed testing methodology SHALL describe the method of achieving all the test phases, defined in Table 14, successfully.			

SOW	[SOW-604]	The Contractor SHALL describe in the MTP how the following objectives will be met: o Compliance with the requirements of the Contract o Verification that the design produces the capability required o Compatibility among internal system components o Compliance with the SRS requirements o Compliance with external system interfaces and/or systems o Confidence that system defects are detected early and tracked through to correction, including re-test and regression approach o Compliance with Purchaser policy and guidance (i.e. security regulations, etc.) o Operational readiness and suitability o Product Quality Criteria (Figure 5: Product Quality Criteria)			
SOW	[SOW-605]	The Contractor SHALL describe the Contractor's test organization and its relationship with the Contractor's Project Management Office and Quality Assurance (QA) functions in the MTP.			
SOW	[SOW-606]	The Contractor SHALL describe in the MTP "Entry and "Exit" criteria for each of the formal TVV events. The Contractor SHALL seek approval of all criteria related to an event not later than the TRR of the event.			
SOW	[SOW-607]	The Contractor SHALL provide in the MTP the schedule, location and scope for all the events to be run, specifying to which phase they belong. When the contractor identifies that multiple events are required for a phase, this SHALL also be specified in the MTP.			
SOW	[SOW-608]	Together with the MTP, the contractor SHALL provide a defect reporting and management process to be applied during the TVV activities in Table 14.			
SOW	[SOW-609]	The Contractor SHALL describe how defects/non-conformances encountered during TVV events will be reported, managed and remedied.			
SOW	[SOW-610]	The MTP SHALL include the Contractor's approach to Test Reviews including Test Readiness Reviews (TRR) and Event Review Meetings (ERM) for each TVV event.			
SOW	[SOW-611]	The Contractor SHALL provide Contractor's provisions and strategy for building/maintaining of the Reference Environment in the MTP.			
SOW	[SOW-612]	The contractor SHALL develop test and use cases to verify and validate all requirements in the SOW, requirements specifications (SRS) and final design. The test cases SHALL follow the template provided by the Purchaser.			
SOW	[SOW-613]	The Contractor developed Test Case/Procedures SHALL clearly describe all the test steps that meet or demonstrate Purchaser's requirements with an expected Test Result and pass/fail result.			
SOW	[SOW-614]	The Contractor SHALL develop test cases and steps for each of the contractual test activities following each type of quality criteria. The Contractor SHALL ensure full test coverage based on a risk analysis and submit them for the Purchaser's review and approval.			
SOW	[SOW-615]	The Contractor SHALL use test tools for development of Test Cases and procedures. Whatever Test tool is used by the Contractor, the output format SHALL fully be compatible, transferrable and usable with the Purchaser's tools.			
SOW	[SOW-616]	The Purchaser will review and provide comments to the Contractor delivered Test Cases, Test Procedures and Test Steps within 4 weeks of receipt. Any updated subsequent versions SHALL follow 4 week review cycle by the Purchaser.			
SOW	[SOW-617]	All the Contractor developed Test Cases, Test Procedures and Test Steps SHALL be approved by the Purchaser prior to their execution.			
SOW	[SOW-618]	If the Contractor produced Test Cases, Test Procedures and Test Steps are not approved by the Purchaser, the execution of relevant testing SHALL be adjusted or delayed accordingly until approved by the Purchaser.			
SOW	[SOW-619]	The purchaser must have the final version of the test cases and Event Test Plan available one (1) week prior to the TRR for a specific TVV event			
SOW	[SOW-620]	Any updates required from the execution of test cases during the each phase SHALL be incorporated into the relevant test cases by the Contractor for use during independent verification, validation and acceptance. If only certain sections are affected, then it SHALL be sufficient to up-date and re-issue those section plus cover sheet with amendment instructions. Should major changes in contents or page re-numbering be needed, then the complete section SHALL be re-issued by the Contractor. All changes SHALL be made with the agreement and approval of the Purchaser			
SOW	[SOW-621]	The contractor SHALL create an Event Test Plan (ETP) per each event detailing all the information required for that event. The ETP SHALL follow the template provided by the Purchaser.			
SOW	[SOW-622]	The Contractor SHALL describe in the event test plan what training (if any) will be provided prior to formal TVV events.			

SOW	[SOW-623]	The Contractor SHALL identify, in the ETP, which environment(s) to be used at each TVV event and the responsibilities for configuration control, operation and maintenance of the environment			
SOW	[SOW-624]	The ETP SHALL describe when an agreement SHALL be reached between the Contractor and the Purchaser on the defect categorization and defect priority of failures encountered, as well as a way forward (if either at the end of each day of a TVV event or at the Event Review Meeting). If agreement is not reached, the disputed items SHALL be escalated to the Purchaser's and Contractors' Project Managers			
SOW	[SOW-625]	The Contractor SHALL record the results for each test called for in the Test Plan in a Test Log (also known as Test Execution Log).			
SOW	[SOW-626]	The test report SHALL follow the template provided by the Purchaser, where the cover sheet SHALL clearly show how many tests passed, failed or were not run.			
SOW	[SOW-627]	Test report SHALL indicate the result of the test cases execution.			
SOW	[SOW-628]	Where the Purchaser or his representative has witnessed the testing, appropriate annotations SHALL be made on each page of the test results to ensure that the test report is a true record of test activities and results as witnessed by the Purchaser, and the whole test report SHALL be signed by the Contractor representative and by the Purchaser representative on completion of that testing.			
SOW	[SOW-629]	The Contractor SHALL produce and maintain the Requirement Traceability Matrix (RTM), which includes all functional and non-functional requirements (respecting Purchaser's provided requirement IDs), to track the TVV status of all requirements throughout the Contract execution (especially during the TVV activities).The RTM SHALL also trace the requirements to the design. It SHALL also define how the requirements will be validated or verified at each of the TVV activities: o The verification method: Inspection, Analysis, Test or Demonstration o Correspondent TVV phase(s) for each requirement o Correspondent Test procedure o Coverage Status o Product release o Identify if covered by COTS, or custom development o Identify any Off-specifications associated with the requirement. o Identify test(s) or test waiver(s) on the basis of which the requirement was demonstrated. o Identify associated problem report for failed requirements			
SOW	[SOW-630]	The Purchaser will review and approve the proposed RTM.			
SOW	[SOW-631]	The contractor SHALL maintain the RTM updated during the project lifecycle.			
SOW	[SOW-632]	The Contractor SHALL provide the Purchaser with updates (via the tools) to the RTM daily during the execution of an event, and following the conclusion of each event defined in Table 14: List of TVV Phases. A workflow for updating the RTM SHALL be proposed by the Contractor and approved by the Purchaser.			
SOW	[SOW-633]	The contractor SHALL include in the RTM (and be able to differentiate from SRS requirements) the requirements derived from the gap analysis of the Operational Acceptance Criteria.			
SOW	[SOW-634]	The Contractor SHALL produce an STVP, to ensure that the Security testing, including verification of compliance with NATO CIS security regulations (in ~~Annex C~~ 2.1.1. Security Documents of the SOW) is applied. This is an integral part of the Independent Verification and Validation process.			
SOW	[SOW-635]	The STVP SHALL support the accreditation of the System Platform. This document SHALL be approved by Security Accreditation Authority (SAA) – Section 10.2.			
SOW	[SOW-636]	The Contractor SHALL generate and deliver automated test procedures/cases compatible with Purchaser test management and automation tools.			
SOW	[SOW-637]	The Contractor SHALL make use of automated testing and supporting testing tools (test management, requirement coverage, defect management, etc.) to the maximum applicable extent, for all system development, implementation, internal and formal tests. The process and proposed supportive tools SHALL be described in the Master Test Plan (MTP). In areas where the Purchaser already uses specific tools, the Contractor SHALL make use of the tools in use by the Purchaser			
SOW	[SOW-638]	Tools supporting requirements coverage, defect management and test management SHALL be selected and hosted by the purchaser and used by the Contractor. For any internal work, the Contractor may use their own internal tools, but the tools used for the contractor's internal work SHALL be able to natively interface with the tools selected and hosted by the Purchaser in order to keep all TVV related data for the project in the purchaser tools.			

SOW	[SOW-639]	The Contractor SHALL conduct testing during the Project lifecycle compliant with the following requirements:			
SOW	[SOW-640]	The Contractor is responsible for conducting all testing during the Project lifecycle. The contractor SHALL provide evidence to the Purchaser of the results of these testing activities. The Contractor SHALL respond to any Purchaser clarification requests regarding test results or performance within two working days.			
SOW	[SOW-641]	The Contractor SHALL conduct all testing activities for any architectural changes.			
SOW	[SOW-642]	The Contractor SHALL support post go-live activities during the Operational Acceptance phase, to evaluate the IEG-C capability performance and establish benchmarks for future enhancements, including any changes made to fulfil the requirements.			
SOW	[SOW-643]	The Contractor SHALL provide status reports to the Purchaser regarding verification and validation activities during the planning/design and development phases, via the use of a dashboard report within the test management tool set and through meetings. The Contractor SHALL provide report(s) to the Purchaser following the completion of any TVV event. The Purchaser will approve the report and its findings within five business days.			
SOW	[SOW-644]	Progress and result measurement SHALL be approved by the Purchaser and focused on KPIs.			
SOW	[SOW-645]	Test results SHALL be recorded in the test management tool set. All results of all formal acceptance testing performed during a given day must be recorded in the test management tool. The Contractor SHALL provide these test results for any given day by the starting of the next business day (0800 AM), but as a minimum not later than 24 hours following the execution of any test.			
SOW	[SOW-646]	The Contractor SHALL conduct a Test Readiness Review (TRR) meeting at least one week prior to the events defined in Table 14: List of TVV Phases. The TRR SHALL ensure that all entry criteria for the events have been met. Documentation that requires review by the Purchaser prior to a TRR, as defined in the Event Test Plan (ETP), SHALL be provided no less than 2 weeks prior to TRR.			
SOW	[SOW-647]	The Purchaser has the right to cancel the TRR and/or any formal test event if the evidence demonstrates that execution of the test event will not be effective.			
SOW	[SOW-648]	The Contractor SHALL demonstrate that all the internal tests and dry runs are successful with test reports and results delivered to the Purchaser at least 2 weeks prior to start of any Contractual test activities.			
SOW	[SOW-649]	The start and/or ending of any test session SHALL be subject to the Purchaser approval. In the event that critical issues are encountered which impact the process of the testing or if the other functions depend on the failed test cases, the Purchaser has the right to stop the testing for Contractor's investigation. The tests can only re-start if Purchaser agrees to continue testing from the point of failure or re-start testing from the beginning.			
SOW	[SOW-650]	The Contractor SHALL convene an Event Review Meeting (ERM) as defined in the ETP and MTP. The ERM SHALL ensure that the event results, defect categorization and a way forward to fixing the defects (if required) is agreed upon the Contractor and the Purchaser as well as any other items identified in the exit criteria defined and agreed for the event. If agreement is not reached, the disputed items SHALL be escalated to the Purchaser's and Contractors' Project Managers. The exit criteria presented in the ERM may as well be utilized as success criteria.			
SOW	[SOW-651]	An event starts with the Test Readiness Review (TRR) and finishes off with the Event Review Meeting (ERM).			
SOW	[SOW-652]	During formal TVV phases, a daily progress debrief SHALL be scheduled. Participation to the daily progress debrief will be agreed between Purchaser and Contractor. The aim of the debrief is to get a common understanding on what tests were run, which passed, which failed, and whatever defects were reported during the day.			
SOW	[SOW-653]	For each TVV event, the Contractor SHALL provide log/record of the event, including but not limited to individual test results, defects found, requirement coverage, test execution durations, deviations during execution and sign-off for each result by both the Contractor and Purchaser.			
SOW	[SOW-654]	The Contractor shall correct and re-test all failures with severity "Critical" or "Major".			
SOW	[SOW-655]	The Contractor shall record the agreed action plan for failures with severity "Moderate", "Minor" and "Cosmetic".			
SOW	[SOW-656]	The Contractor shall fix and demonstrate that the recorded issues or faults are fixed and working correctly. The next contractual test activity shall not start until all the findings are fixed to the Purchaser's satisfaction.			
SOW	[SOW-657]	At the end of the project, the Contractor SHALL provide the final version of all artefacts (regardless of format) created during the execution of all TVV activities.			
SOW	[SOW-658]	The Contractor SHALL obtain the approval of the Purchaser regarding the environments the formal events will take place on and in requesting the approval, indicate what support is required from the Purchaser to configure and prepare the environment. This includes any data from the Purchaser required for the test event. The Reference Environment Configuration SHALL be formally controlled using configuration management tools, and each baseline that will enter into a contractual event SHALL be delivered to the Purchaser for approval prior to TRR.			

SOW	[SOW-659]	The Contractor SHALL ensure that all test/reference environments are under proper configuration management, especially configuration control. The Configuration Management toolset and process SHALL be approved by the Purchaser.			
SOW	[SOW-660]	The Contractor may request a Test Waiver if the Contractor has previously successfully completed qualification testing to national, or international standards for assemblies, subassemblies components or parts. The Purchaser, after review of test waivers and analysis of their impact, reserves the right to require test and certification of the modified equipment at no cost to the Purchaser. The Purchaser has the right to reject any test Waiver.			
SOW	[SOW-661]	In respect to a requested waiver, the Contractor SHALL certify that the test environment to be implemented is identical to that which was originally used for testing, or advise the Purchaser of design/construction changes which affect form, fit or function.			
SOW	[SOW-662]	The Contractor SHALL record and log all waiver requests along with their resolution submitted for the Purchaser's approval.			
SOW	[SOW-663]	In the event of failed TVV event and the need to return to a site for re-testing; travel and per diem expenses of NATO personnel SHALL be borne by the Contractor			
SOW	[SOW-664]	The Contractor SHALL use the Purchasers' categorization nomenclature for all defects and non-compliances			
SOW	[SOW-665]	Should a failure be identified during a TVV event/activity, a defect SHALL be recorded in the Agency's' test management and defect management systems. Once the event has concluded, the defect SHALL be reviewed during the event review meeting to agree on the severity, priority and category. The event test report SHALL then report the disposition of all defects recorded during the event and the defect management system SHALL be updated accordingly. Classification SHALL follow Table 16: Definitions for Defect Categorization, Table 17: Classification of defects based on severity, Table 18: Priority Classes for Defect Classification and Table 19: Deficiency Categories .			
SOW	[SOW-666]	According to their severity, defects SHALL be classified as one of the following in Table 17: Classification of defects based on severity: Critical Major Moderate Minor Cosmetic			
SOW	[SOW-667]	According to their priority, defects SHALL be classified as one of the following in Table 18: Priority Classes for Defect Classification: Urgent Medium Low			
SOW	[SOW-668]	According to their category, deficiencies SHALL be classified as one of the following in Table 19: Deficiency Categories: Defect Enhancement Document Clarification Waiver			
SOW	[SOW-669]	The Contractor SHALL respect requirements below for every site survey.			
SOW	[SOW-670]	For each site survey, the Contractor SHALL conduct site survey preparatory work, visit each site subject to site survey, survey relevant facilities, interview site personnel, and collect data to support project activities.			
SOW	[SOW-671]	The Contractor SHALL ensure coherence between site survey results and project documentation (e.g., System Design Documentation Package, SIP) at any time. The Contractor SHALL update project documentation accordingly.			
SOW	[SOW-672]	The Contractor SHALL prepare a SSWB of checklists, fill-in forms, installation sketches, contact information, installation specifications, and site data to be collected by the Contractor during the site survey, and any other documentation required to perform site surveys.			
SOW	[SOW-673]	The Contractor SHALL make the SSWB available for Purchaser review and comment before the first site survey, and SHALL maintain and update as necessary during the site survey process.			

SOW	[SOW-674]	Upon acceptance of the SSWB by the Purchaser, the Contractor SHALL distribute the SSWB to the site(s) for preparation of the Site Surveys. This approach will enable a better preparation by the sites.			
SOW	[SOW-675]	The Contractor's site survey(s) and installation sequence and dates reflected in the Project Implementation Plan SHALL be co-ordinated by the Contractor with the Purchaser and the Site POC to accommodate site-specific requirements, exercises, holiday periods, and other considerations.			
SOW	[SOW-676]	The Contractor SHALL prepare and provide an Introductory Briefing as an introduction to the IEG-C project, which will not assume other than basic knowledge of the project by the site personnel, covering at least: o An outline of the system requirements, o System functionalities, o The sites to be implemented, o The project timelines, o The goals and objectives and agenda of the Site Survey process, o The notional implementation identified for the surveyed site, to be refined through the Site Surveys activities.			
SOW	[SOW-677]	At the beginning of the site survey the Contractor SHALL provide a presentation to the local site personnel on the objectives and conduct of the site visit in the context of the overall IEG-C project.			
SOW	[SOW-678]	During the Site Surveys activities the Contractor SHALL determine the necessary installation preparations and support arrangements and collect all system implementation-relevant information. This SHALL include: o Identification of the IEG-C IEG-C Administrators, CIS Security Administrators, Operators, and more generally all Points of Contact; o Identification of existing business processes (for both physical access control and logical access control), and how those processes will integrate with IEG-C Capability. o Identification of the system IEG-C will interface with, in accordance with the business processes and transition requirements from existing capabilities to the IEG-C Capability; o Identification of the system that are not ready to be migrated to IEG-C; o Analysis of the training needs (see also 11.7); o Identification of any input (item of equipment, documentation, information) or work required from the Purchaser and from the Site with indication of suspense date; o Identification of the facilities where the IEG-C will have to be installed, together with each facility's zone level (see [NCIA AI TECH 06.03.01, 2015]); o Identification of any potential TEMPEST-related requirement for the IEG-C equipment(see [NCIA AI TECH 06.03.01, 2015]); o List of all system CIs (nature and quantities) to be installed in the site o Update of the user list (see ANNEX B) o Identification of the tools, policies and procedures in use at Purchaser facilities, in order to determine the integration requirements with the ITSM tools.			
SOW	[SOW-679]	After the Site Survey the Contractor SHALL present to the Purchaser his site engineering and installation drawing(s) and identify actions and follow-on activities.			
SOW	[SOW-680]	The Contractor SHALL determine if site-specific equipment is required at a location as part of any Site Survey performed under this Contract.			
SOW	[SOW-681]	If site-specific equipment is required, the Contractor SHALL issue an Engineering Change Proposal (ECP).			
SOW	[SOW-682]	In the ECP, the Contractor SHALL identify any requirements of the IEG-C System Design Specification it believes will not be met due to differences between the site-specific equipment and the standard baseline.			
SOW	[SOW-683]	If these exceptions to the IEG- System Design Specification are accepted by the Purchaser and incorporated into the Contract as formal amendments, the Contractor is not required to demonstrate, as part of its Site Activation work, that the associated System Design Specification requirement has been met. In such a case, the Contractor SHALL update the System Design Specification to reflect site-specific situations.			

SOW	[SOW-684]	The Contractor SHALL identify all facilities support, including modifications or additions, required. After coordination with the Purchaser, this notification SHALL be in the form of a letter to the site POC, with a copy to the Purchaser, accompanied by engineering drawings, checklists, or any other supporting information. Facilities support issues that represent Medium or High risk items SHALL be reflected in the Risk Log.			
SOW	[SOW-685]	The Contractor SHALL produce and deliver a Site Survey Report for each site. detailing its findings from the site survey, identifying all required Purchaser and Contractor actions to prepare for, conduct, or support IEG-C installation and activation, and identifying the type of training courses required and the number of Purchaser staff to be trained for each course.			
SOW	[SOW-686]	The Contractor SHALL accurately and formally document the findings of the Site Survey and the preparatory work required from the Site.			
SOW	[SOW-687]	After the Site Survey the Contractor SHALL present to the Purchaser his site engineering and installation drawing(s) and identify actions and follow-on activities.			
SOW	[SOW-688]	The Contractor's Site Survey Reports SHALL be provided within one week after the respective Site Survey is completed.			
SOW	[SOW-689]	At minimum, the Site Survey Report SHALL include:			
SOW	[SOW-690]	At the end of the site survey the Contractor SHALL provide an out brief on the outcome of the site survey and identify actions and follow-on activities.			
SOW	[SOW-691]	The platform SHALL demonstrate compliance with the NATO Security Policy and supporting directives and IEG-C security accreditation document set by obtaining the security accreditation of interconnections via the IEG-C installations.			
SOW	[SOW-692]	The Contractor SHALL be responsible to follow, implement and conform to the Pre-Accreditation Activities, and the Accreditation Process as defined and documented in [AC/35-D/2005-REV3] and Security Accreditation Plan (SAP) for IEG-C in order to obtain the required security accreditation statement(s) for the interconnections via IEG-C during each phase of the IEG-C project.			
SOW	[SOW-693]	The Contractor SHALL be required to carry out and meet the terms of the Security Accreditation Authority to perform any Post-Accreditation activities, such as periodic re-assessments of the security risks and periodic inspections up to the time of handover of the IEG-C to the CIS Provider (CISP).			
SOW	[SOW-694]	The Contractor SHALL obtain Approval for Testing (AfT) and/or Interim Security Accreditation (ISA) which are necessary during the stages of the implementation, tests and trials of the IEG-C project. This does not diminish the requirement for the Contractor to obtain the full Security Accreditation statement for each interconnection via IEG-C.			
SOW	[SOW-695]	The Contractor SHALL take action to follow, carry out the necessary work and to implement the advice, instructions and changes given by the SAA and local SAA's for the IEG-C.			
SOW	[SOW-696]	The Contractor SHALL produce security accreditation documentation and/or provide inputs to documents in support of the 3.7 Acceptance of IEG-C security accreditation package , as detailed in Security Accreditation Plan (SAP) for IEG C			
SOW	[SOW-697]	The Contractor SHALL produce all security accreditation documentation or inputs to documents using security document templates provided by the Purchaser. These will be provided after the Contract Award.			
SOW	[SOW-698]	The Contractor SHALL be responsible to implement the activities described in the SAP as approved by the SAA.			
SOW	[SOW-699]	The Contractor SHALL update the initial CIS description document based on the System Description in Section 1.2 provided by the Purchaser, including all relevant information taken from the System Design Documentation Package and adapted to the SAA needs.			
SOW	[SOW-700]	The Contractor SHALL address Purchaser comments (including SAA comments) to achieve CIS description endorsement by the SAA.			
SOW	[SOW-701]	The Contractor SHALL maintain the CIS description during the project.			
SOW	[SOW-702]	The Contractor SHALL develop the SRA in accordance with Guidelines for Security Risk Management of CIS (Ref. [AC/35-D/1017-REV3]).			
SOW	[SOW-703]	The Contractor SHALL use the NATO template [SRA template] to document the results of the SRA.			
SOW	[SOW-704]	The Contractor SHALL identify areas of the IEG-C requiring safeguards and countermeasures to comply with NATO Security Policy and supporting directives and [NS Reference Baseline]. The decision on specific security mechanisms will be based on evidence and results produced by the Security Risk Assessment.			
SOW	[SOW-705]	The Contractor SHALL consider any change to be within the technical and financial scope of this Contract whenever the implementation of security measures results in the modification of the design (without introducing additional components), other documentation requirements, and changes to configuration of components; no ECP SHALL be generated.			
SOW	[SOW-706]	The Contractor SHALL raise an ECP whenever the implementation of security measures results in a requirement for additional components to be procured for implementation that could not be reasonably foreseen beforehand.			
SOW	[SOW-707]	The Contractor SHALL address Purchaser comments (including SAA comments) to achieve SRA report approval by the SAA.			

SOW	[SOW-708]	The Contractor SHALL maintain the SRA report during the project.			
SOW	[SOW-709]	The Contractor SHALL produce a generic System Interconnection Security Requirement Statement (SISRS) for IEG-C to include the minimum requirements mandated by NATO Security Policy and supporting directives and security measures to counter the risks identified in the IEG-C SRA.			
SOW	[SOW-710]	The Contractor SHALL produce the SISRS template for IEG-C using and following the guidance provided by the Purchaser.			
SOW	[SOW-711]	The Contractor SHALL ensure that each security requirement in the SISRS have a unique identifier which is crossed referenced to the security mechanism (Ref. [NS Reference Baseline]) addressing the requirement.			
SOW	[SOW-712]	The Contractor SHALL describe in detail possible information exchange scenarios and relevant security mechanisms implemented.			
SOW	[SOW-713]	The Contractor SHALL address Purchaser comments (including SAA comments) to achieve generic SISRS approval by the SAA.			
SOW	[SOW-714]	The Contractor SHALL maintain the generic SISRS during the project.			
SOW	[SOW-715]	The Contractor SHALL produce specific procedures for centralized management of IEG-C and include them in IEG-C-specific section of the Security Operating Procedures (SecOPs) for Gateway Services Section.			
SOW	[SOW-716]	The Contractor SHALL address Purchaser comments (including SAA comments) to part of the SecOPs related to IEG-C.			
SOW	[SOW-717]	The Contractor SHALL produce the Security Test & Verification Plan (STVP) for the IEG-C using the NATO template [STVP template], defining the set of test procedures to prove that the security mechanisms designed into the IEG-C enforce the security requirements identified in the IEG-C SISRS. Each test procedure SHALL have unique ID and refer to at least one requirements from IEG-C SISRS and at least one Security Mechanism (from [NS Reference Baseline]).			
SOW	[SOW-718]	The Contractor SHALL provide traceability matrix to ensure every security test to be cross referenced to the corresponding security requirement from SISRS as well as to the tested security mechanisms.			
SOW	[SOW-719]	The Contractor SHALL ensure all security mechanisms of the IEG-C to be planned for testing.			
SOW	[SOW-720]	The Contractor SHALL address Purchaser comments (including SAA comments) to achieve STVP approval by the SAA.			
SOW	[SOW-721]	The Contractor SHALL maintain the STVP during the project.			
SOW	[SOW-722]	Where necessary due to local security requirements, the Contractor SHALL develop local version of STVP to address local security requirements (e.g. from [AD 070-005]).			
SOW	[SOW-723]	For each IEG-C site, the Contractor SHALL execute security testing in accordance with STVP (or its local version, where relevant) and in coordination with the Purchaser.			
SOW	[SOW-724]	For each IEG-C site the Contractor SHALL generate a Security Test and Verification Report, containing results of all security tests specified in the STVP, using the STVR template.			
SOW	[SOW-725]	The Contractor SHALL ensure security test identifiers are preserved in the Report as defined in the STVP or relevant local STVP.			
SOW	[SOW-726]	The Contractor SHALL complete Statement of Compliance for each interconnection via IEG-C. The Statement of Compliance SHALL address local security requirements, where applicable.			
SOW	[SOW-727]	The Contractor SHALL ensure draft versions of security documents are provided by the PDR (EDC+3MO) and final versions by the CDR (EDC+6MO).			
SOW	[SOW-728]	The Contractor SHALL ensure implementation plans are flexible to take account of the time required for accreditation.			
SOW	[SOW-729]	The Contractor SHALL undertake the work identified in the column 'Contractor Responsibility' in Table 18: Security Accreditation Documentation and Contractor Responsibility below:			
SOW	[SOW-730]	The Contractor SHALL establish, execute, document and maintain an effective Quality Assurance (QA) programme throughout the Contract's lifetime.			
SOW	[SOW-731]	The Contractor's QA effort SHALL apply to all services and all products (both management products and specialist products) to be provided by the Contractor under this contract (this includes all hardware and software – COTS as well as developed for this project – documentation and supplies that are designed, developed, acquired, maintained or used, including deliverable and non-deliverable items).			
SOW	[SOW-732]	The Contractor's QA effort SHALL ensure that procedures are developed, implemented and maintained to adequately control the design, development, production, purchasing, installation, inspection, testing, configuration management and customer support of all services and all products (both management products and specialist products), in accordance with the requirements of this Contract.			
SOW	[SOW-733]	The Purchaser, in this contract, applies the NATO Standardisation Agreement, STANAG 4107 "Mutual Acceptance of Government Quality Assurance and usage of the Allied Quality Assurance Publications (AQAP)" (see 2.1.2) which the Contractor SHALL herewith accept and adhere to.			

SOW	[SOW-734]	The Purchaser may delegate the Quality Assurance to the appropriate Government Quality Assurance Authority (GQAA) in accordance with STANAG 4107. The Purchaser, through its own Quality Assurance, however, will retain the overall supervisory and liaison authority concerning all Quality related matters, and, for this purpose, will use its own QA Personnel.			
SOW	[SOW-735]	The term "NATO Quality Assurance Representative" (NQAR) SHALL apply to any of the Purchaser appointed Quality Assurance Representative, whether nominated by the GQAA or by Purchaser QA. During the entire contract implementation, the NQAR(s) within their own rights, defined in the contract applicable AQAPs, SHALL assure the Contractor's and Sub-Contractor's compliance with all Quality related contractual requirement.			
SOW	[SOW-736]	The term "Contractor Quality Assurance Representative" (CQAR) SHALL apply to any of the Contractor appointed Quality Assurance Representative. That person SHALL be designated as the Contractor's QA Representative and point of contact for interface with and resolution of quality matters raised by the NCI Agency or his delegated NQAR and identified in the Quality Assurance Plan.			
SOW	[SOW-737]	The Contractor SHALL be responsible for controlling product quality and for offering to the NQAR(s) for acceptance only those supplies and services which conform to contractual requirements and, when required, for maintaining and furnishing objective evidence of this conformance.			
SOW	[SOW-738]	The NQAR(s) is (are) responsible for determining that contractual requirements have been complied with, prior to the acceptance of the services.			
SOW	[SOW-739]	The Contractor SHALL give written notice to the NQAR(s) at least four weeks in advance that the services are being presented for inspection, testing and acceptance. Testing SHALL only be permitted by using Purchaser approved test procedures and plans.			
SOW	[SOW-740]	The Contractor SHALL establish, document and maintain a Quality Management System in accordance with the requirements of ISO 9001:2015.			
SOW	[SOW-741]	The Contractor's and Sub-Contractor's QMS relevant to performance under this contract SHALL be subject to continuous review and surveillance by the cognizant NQAR(s).			
SOW	[SOW-742]	The Contractor SHALL include in orders placed with his Sub-Contractor(s) and Supplier(s), the QMS requirements necessary to ensure the supplies and services covered by the Sub-contract(s) and/or Purchase Orders conform to the requirements of the prime contract. As required, STANAG 4107 SHALL be specified.			
SOW	[SOW-743]	The Contractor SHALL specify in each order placed with his sub-Contractor(s) and Supplier(s),the Purchaser's and his NQAR(s) rights of access to all premises where contractual work is performed, in order to carry out audits, inspections, tests and other functions as may be required by the NQAR(s).			
SOW	[SOW-744]	The Contractor's QA effort SHALL be described in detail in a Quality Assurance Plan (QAP), which SHALL clearly indicate the QA activities, responsibilities, and checks for the Contractor and any Sub-Contractors.			
SOW	[SOW-745]	All versions of the QAP SHALL be configuration controlled and provided to the Purchaser for acceptance.			
SOW	[SOW-746]	The acceptance of the QAP by the Purchaser signifies only that the Purchaser agrees to the Contractor's approach in meeting the requirements. This acceptance in no way relieves the Contractor from its responsibilities to meet the requirements stated in this Contract.			
SOW	[SOW-747]	The Contractor SHALL review his QA programme periodically and audit it for adequacy, compliance and effectiveness.			
SOW	[SOW-748]	The Contractor SHALL ensure that all contractual requirements, including NATO supplements, are included in internal audits.			
SOW	[SOW-749]	The Contractor SHALL inform the NQAR(s) of deficiencies identified during internal audit unless otherwise agreed between the NQAR and/or the Purchaser and the Contractor.			
SOW	[SOW-750]	The Contractor SHALL include a risk management section within the QAP including the risks connected to the subcontractors of the Contractor.			
SOW	[SOW-751]	The Contractor SHALL agree to provide all necessary assistance to the NQAR.			
SOW	[SOW-752]	The Contractor SHALL make his quality records, and those of his subcontractors, available for evaluation by the NQAR throughout the duration of the Contract.			
SOW	[SOW-753]	The Contractor SHALL use the review processes described in the Configuration Management Plan (CMP) to manage changes to the QAP.			
SOW	[SOW-754]	The Contractor SHALL update the document, as required, from the delivery date of the initial QAP through Final Operating Capability (FOC), under Configuration Management. The Contractor SHALL provide a copy of each new version of the QAP to the NQAR and the new version SHALL be approved by the Purchaser.			
SOW	[SOW-755]	If the Contractor becomes aware at any time before acceptance by the Purchaser that a defect exists in any supplies, the Contractor SHALL coordinate with the Purchaser and promptly correct the defect.			

SOW	[SOW-756]	The Contractor SHALL implement a quality/product assurance risk log/action tracking system, which identifies all the major/minor non conformity raised during the life cycle of this Contract.			
SOW	[SOW-757]	The Contractor, through its Corrective Action System, SHALL track all reported and recorded problems and deficiencies until their closure and clearance.			
SOW	[SOW-758]	The Contractor SHALL notify the Purchaser of proposed action, resulting from Review Output that will affect compliance with contractual requirements.			
SOW	[SOW-759]	The Contractor SHALL demonstrate that all the non-conformities are solved and all defects are closed before the product acceptance.			
SOW	[SOW-760]	The Contractor SHALL issue and implement documented procedures which identify, control and segregate all non-conforming products. Documented procedures for the disposition of non-conforming product are subject to approval by the Purchaser when it can be shown that they do not provide the necessary controls.			
SOW	[SOW-761]	The Contractor SHALL notify the Purchaser of non-conformities and corrective actions required, unless otherwise agreed with the Purchaser.			
SOW	[SOW-762]	When the Contractor establishes that a subcontractor or a Purchaser Furnished Equipment (PFE) product is unsuitable for its intended use, he SHALL immediately report to and coordinate with the Purchaser the remedial actions to be taken.			
SOW	[SOW-763]	The Contractor SHALL ensure that only acceptable products, intended for delivery, are released. The Purchaser reserve the right to reject non-conforming products.			
SOW	[SOW-764]	The Contractor SHALL document the Corrective Action System in the QAP.			
SOW	[SOW-765]	The Contractor SHALL describe the process used for defect management in the QAP.			
SOW	[SOW-766]	The Contractor SHALL deliver all the CoCs for COTS software (including firmware) and hardware released by the COTS Vendors.			
SOW	[SOW-767]	The Contractor SHALL provide a CoC at release of product to the Purchaser unless otherwise instructed.			
SOW	[SOW-768]	The Contractor SHALL make all support tools available for demonstration to the NQAR, upon request.			
SOW	[SOW-769]	The Contractor SHALL also make available to the Purchaser for review upon request, associated records and documentation, including but not limited to, control, authorization for use, calibration, validation, qualification, as applicable, per respective contract requirement.			
SOW	[SOW-770]	The Contractor SHALL implement a CM process as referred to in [STANAG 4427, 2014], [ACMP-2000, 2017], [ACMP 2009, 2017] and [ACMP-2100,2017] to carry out the Configuration Management functions as described in this SOW (configuration item identification, configuration control, configuration status accounting, and configuration audit and verification).			
SOW	[SOW-771]	The Contractor SHALL ensure that an effective Configuration Management organization is established to implement and manage the Configuration Management processes throughout the duration of this contract.			
SOW	[SOW-772]	The Contractor SHALL create and maintain four Configuration Baselines, as follows (see Figure 3). The Contractor shall create multiple instances of one type of the configuration baseline to adjust to the agile delivery approach, as required. • Functional Baseline (FBL, or “as required”), • Allocated Baseline (ABL, or “as designed”), • Product Baseline (PBL, or “as built”), • Operational Baseline (OBL, or “as delivered”, or “as deployed”).			
SOW	[SOW-773]	Under the CM program the Contractor SHALL maintain and update all project CIs as required by changes within the project or external to the project throughout the duration of the contract.			
SOW	[SOW-774]	The Contractor SHALL ensure that all system configuration and baselines will be detailed in a System Version Definition Document (SVDD); see Section 15.7.			
SOW	[SOW-775]	The Contractor SHALL ensure that there is full traceability through all baselines back to the functional baseline.			
SOW	[SOW-776]	The Contractor’s developed baselines SHALL be encapsulated and maintained by the Contractor in a CM database (CMDB) established by the Contractor as specified under Configuration Management Tools.			
SOW	[SOW-777]	The Contractor SHALL develop and derive the FBL from the IEG-C SRS and SHALL establish the FBL at the successful completion of the SRR (EDC+2MO) with the approved updated SRS.			
SOW	[SOW-778]	The Contractor SHALL maintain an up-to-date version of the Functional Baseline in the CMDB and ensure the relevant project documentation such as Requirements Traceability Matrix (RTM) is updated based on the approved FBL. The information SHALL be integrated into the NCI Agency DOORS database.			

SOW	[SOW-779]	The Contractor's developed design in the ABL SHALL meet the functional and non-functional requirements allocated in the FBL.			
SOW	[SOW-780]	The ABL set of documents and artefacts SHALL contain, but is not limited to, the following documents: o System Design Specification o Interface Control Document (ICD) o The Test Specification o Requirements Traceability Matrix			
SOW	[SOW-781]	The Contractor's initial ABL SHALL be established first at the successful completion of the PDR (EDC+3MO) and SHALL be finally accepted at the successful completion of CDR (EDC+6MO).			
SOW	[SOW-782]	The Contractor SHALL maintain and update the ABL configuration during the System Baseline Reviews (SBR).			
SOW	[SOW-783]	The Contractor SHALL ensure its PBL meets the functional and non-functional requirements allocated in the FBL and the design of the ABL.			
SOW	[SOW-784]	The Contractor SHALL ensure its PBL products are distinguished in documentation, software, hardware/equipment and services.			
SOW	[SOW-785]	The Contractor SHALL ensure the products of its PBL contain, but are not limited to, the following: o Hardware components, including COTS, o Software media, including COTS, o Software license(s), including COTS.			
SOW	[SOW-786]	The Contractor SHALL ensure its PBL (supporting) documentation products contain, but are not limited to: o As-built drawings, o COTS O&M manuals, o FBL documentation, o ABL documentation, o O&M manuals (custom), o Inventory documentation (both for hardware and software products), o Software Distribution list (SWDL), o Training documentation, o QA documentation, o Security documentation, o Configuration Management Database including the individual artefacts, o Warranty documentation o Requirements Traceability matrix.			
SOW	[SOW-787]	The Contractor SHALL include the SDS (including the RTM), the Test Plan, and any other documentation deemed appropriate by the Contractor, in accordance with provisions of IEEE 12207, to ensure requirements are reflected in the system during development and integration, can be demonstrated through a comprehensive set of tests, and can be delivered in the form of the Product Baseline.			
SOW	[SOW-788]	The IEG-C PBL SHALL be initially established before the testing events and SHALL be updated after the changes applied based on the outcomes of the testing events.			
SOW	[SOW-789]	The Contractor SHALL include in the PBL release package the following elements, as a minimum all items described in Table 19: Content for Product Baseline Release Package			
SOW	[SOW-790]	The Contractor's developed OBL SHALL be initially established after successful completion of the PSA (EDC+20mo) and then finally established after successful completion of FSA. It reflects the "as-deployed" configuration of the system.			
SOW	[SOW-791]	The Contractor's OBL SHALL be established site-specific, as applicable.			
SOW	[SOW-792]	The Contractor's OBL SHALL contain, but is not limited to: o All delivered software CI (i.e. CSCI, CSC, CSUs), including COTS; o All delivered hardware CI (if any); o All the Documentation that comprise the system and any subsequent releases;			

SOW	[SOW-793]	IEG-C Baselines SHALL be given a major release number and a minor release number comprising an X.X notation. The complete baseline identifier SHALL include the specific baseline identifier (i.e. FBL, ABL, PBL, and OBL), site identification (if applicable) and security domain difference (if applicable). Final numbering scheme for the baseline identification may be modified with Purchaser agreement, and it SHALL be proposed for Purchaser approval within the CM Plan.			
SOW	[SOW-794]	The Contractor SHALL update and re-release the PBL documentation outlined in Table 4, as required.			
SOW	[SOW-795]	The Contractor SHALL provide a CMP tailored to the requirements of the proposed technical solution.			
SOW	[SOW-796]	The Contractor’s CMP SHALL be structured as a living document subject to revisions and updates, as required.			
SOW	[SOW-797]	The Contractor SHALL place the plan under configuration control prior to its implementation and for the life of the Contract.			
SOW	[SOW-798]	In producing the CMP, the Contractor SHALL define the organisation and procedures used to configuration manage the functional and physical characteristics of CIs, including interfaces and configuration identification documents.			
SOW	[SOW-799]	The Contractor SHALL ensure that all required elements of CM are applied in such a manner as to provide a comprehensive CM process.			
SOW	[SOW-800]	The Contractor’s CM Plan SHALL be compatible and consistent with all other plans, specifications, standards, documents and schedules.			
SOW	[SOW-801]	The Contractor SHALL propose in the CMP detailed configuration control procedures.			
SOW	[SOW-802]	All Contractor and Purchaser activities and milestones related to CM SHALL be identified and included in the PMS of the PMP.			
SOW	[SOW-803]	The Contractor SHALL establish and maintain product-based planning which SHALL include as a minimum: o A product description of the final product of the project; o A Project PBS; o Product Descriptions of each product; o A PFD.			
SOW	[SOW-804]	The Contractor’s CM Plan SHALL address all disciplines within this Section and SHALL as a minimum include, but not be limited to the following Sections: o Introduction; o Organisation; o Configuration Identification and Documentation; o Configuration Control; o Configuration Status Accounting; o Configuration Audits; o Configuration Management Database (CMDB); o Configuration Management tools/Interface management.			
SOW	[SOW-805]	The Contractor SHALL divide the products and specialist products into Configuration Items (CIs).			
SOW	[SOW-806]	The Contractor's CI structure SHALL show the relationships between the lower level Baselines and CIs.			
SOW	[SOW-807]	The Contractor SHALL propose appropriate CIs in the CM Plan including an explanation of the rational and criteria used in the selection process, based on the criteria for selection of CIs as detailed in [ACMP 2009, 2017].			
SOW	[SOW-808]	The Contractor's CIs SHALL be chosen in a way to assure visibility and ease of management throughout the development effort and the support to the OBL after acceptance.			
SOW	[SOW-809]	All Contractor's COTS, adapted, and developed software SHALL be designated as CIs.			
SOW	[SOW-810]	Where Contractor's COTS can be installed in a modular fashion, the description of the CI SHALL unambiguously identify the complete list of installed components.			
SOW	[SOW-811]	The Contractor SHALL designate as CIs all hardware elements (if any) down to the maintenance significant item level.			
SOW	[SOW-812]	The Contractor SHALL ensure the level of granularity for the CI selection reaches at a minimum:			
SOW	[SOW-813]	The Hardware CI attributes SHALL include, but is not limited to, the MDS information,(Optional);			
SOW	[SOW-814]	The Software CI attributes SHALL include, but is not limited to, the [ACMP 2009, 2017] definitions;			
SOW	[SOW-815]	Any Documentation CI that is not linked to a Software CI or Hardware CI (optional) SHALL include, but is not limited to, the Contract SSS attributes.			

SOW	[SOW-816]	The Contractor SHALL be responsible for issuing in a timely manner all approved changes and revisions to the functional, development and PBL documents included in the Contract. This includes changes originated both by the Contractor and the Purchaser.			
SOW	[SOW-817]	Where a change affects more than one document, or affects documents previously approved and delivered, the Contractor SHALL ensure that the change is properly reflected in all baseline documents affected by that change.			
SOW	[SOW-818]	The Contractor SHALL appropriately reflect all design changes in the technical documentation by the issue of appropriate changes or revisions.			
SOW	[SOW-819]	The Contractor SHALL provide all such changes/revisions to the Purchaser.			
SOW	[SOW-820]	The Contractor SHALL be fully responsible for the Configuration Control of all baselines and CIs in accordance with [ACMP 2009, 2017] and [ACMP-2000, 2017].			
SOW	[SOW-821]	The Contractor SHALL define the responsibilities and procedures used within the Contractor's organization for configuration control of established CI, and for processing changes to these CI.			
SOW	[SOW-822]	The Contractor SHALL define the Configuration Baseline Change procedures and SHALL submit Notice of Revision or Request for Deviations (RFD) and Request for Waivers (RFW) when required and approved by the Purchaser.			
SOW	[SOW-823]	The Contractor SHALL provide read-only access to the Purchaser to audit and control its productions environments and configuration management tools (for software, documentation and hardware, if applicable).			
SOW	[SOW-824]	The Contractor SHALL process changes to the his developed baselined CIs as either Class I or Class II ECPs as defined in [ACMP 2009, 2017] and the change request requirements specified.			
SOW	[SOW-825]	The Contractor SHALL use the configuration control procedures specified in the CM Plan for the preparation, submission for approval implementation and handling of ECPs to baselined CIs.			
SOW	[SOW-826]	When submitting ECPs, the Contractor SHALL assign a priority rating of Emergency, Urgent or Routine Extensions to the target times for processing.			
SOW	[SOW-827]	Changes to baseline CIs SHALL be processed as either Class I or Class II ECPs as defined in [ACMP 2009, 2017].			
SOW	[SOW-828]	Class I ECPs SHALL have to be mutually agreed upon by the Contractor and Purchaser.			
SOW	[SOW-829]	Prior to implementation, all Class II ECPs SHALL be submitted by the Contractor to the Purchaser for review and classification concurrence.			
SOW	[SOW-830]	If the Purchaser’s representative does not concur in the classification, Class I ECP procedures SHALL be applied by the Contractor and the ECP and then formally submitted to the Purchaser for approval or rejection.			
SOW	[SOW-831]	Extensions to the target times for processing Class I ECPs SHALL be mutually agreed upon by the Contractor and Purchaser.			
SOW	[SOW-832]	The Contractor SHALL not implement Class I ECPs before Purchaser approval.			
SOW	[SOW-833]	The Contractor SHALL reflect in the technical documentation all design changes appropriately by the issue of appropriate documentation revisions.			
SOW	[SOW-834]	The Contractor SHALL provide all supporting documentation and information to detail the impact of the change in design, specification, maintenance and support, documentation, cost, schedule, and security, as requested by the Purchaser.			
SOW	[SOW-835]	The Contractor SHALL propose in the CM Plan an ECP format based on the requirements in [ACMP 2009, 2017].			
SOW	[SOW-836]	The Contractor SHALL include in an ECP as a minimum, the following information: o Reference Number; o Requirement affected (using the outline numbering of the core SOW, or of Annex A); o Nature of change; o Rationale for the change; o Impact of change; o Description of how the change will be reflected in the delivered system's cost, schedule, and/or performance. This description SHALL include any trade-offs that SHALL be considered; o Status; o Priority.			

SOW	[SOW-837]	After the completion of Deployment Authorization (DA at EDC+20mo), the Contractor SHALL provide the ECP's for proposed changes which will also require the new approval for the DA. For that purpose, the Contractor SHALL provide all the information necessary and support the Purchaser Project Manager by any means to obtain the Deployment Authorization based on the proposed change and new baseline.			
SOW	[SOW-838]	The Contractor SHALL comply and support Purchaser's internal Change Management Process in order to obtain the Deployment Authorization Approval through the Change Advisory Board (CAB).			
SOW	[SOW-839]	The Contractor SHALL support the Purchaser in preparing the Request For Change (RFC) to meet the requirements of the Purchaser's Change Evaluation process.			
SOW	[SOW-840]	The Contractor SHALL provide all necessary documentation and information for the successful completion of the Deployment Authorization.			
SOW	[SOW-841]	The contractor SHALL assist the Purchaser with the installation and configuration the system/application in accordance with the Contractor provided Installation and Configuration Manual(s).			
SOW	[SOW-842]	The Contractor SHALL conduct a Functional Configuration Audit (FCA) and deliver the associated FCA report			
SOW	[SOW-843]	After the successful testing of SIT/SAT/UAT and Security tests, the Contractor, through the NATO assigned PM, SHALL submit the baseline to the Purchaser IT Change Management process by submitting the RFC.			
SOW	[SOW-844]	The NATO assigned PM SHALL seek the authorization of deployment on the relevant targeted NATO networks. The Contractor SHALL provide the required final RFC documents (i.e. ECP and supporting documentation) described in SOW 12.6.			
SOW	[SOW-845]	The RFC SHALL be submitted to Purchaser's Change Advisory Board (CAB) for screening. The CAB SHALL decide if further or other tests are required. The latest Purchaser approved baseline for the RFC process SHALL be used.			
SOW	[SOW-846]	If the Contractor is produced a new build or baseline version the Contractor SHALL follow Purchaser's internal Change Management process and test activities as deemed necessary by the CAB.			
SOW	[SOW-847]	The Contractor SHALL note that system implementation activities in operational environment will not start until the DA milestone is approved by the Purchaser.			
SOW	[SOW-848]	The Contractor SHALL provide and update all related baseline documentation and traceability to reflect the modifications triggered by the change.			
SOW	[SOW-849]	The Contractor, if requested by the Purchaser SHALL install the new baseline or other instances of new baselines for Security and other Purchaser related tests.			
SOW	[SOW-850]	The Contractor SHALL supply the documents in Final form listed in Table 20 - System Submission Requirements Matrix (SSRM) for inclusion in the Purchaser Release Package for the RFC.			
SOW	[SOW-851]	If required, the Contractor SHALL prepare, handle, and submit for Purchaser's approval, RFDs and RFWs as defined in [ACMP 2009, 2017].			
SOW	[SOW-852]	The Contractor SHALL propose in the CM Plan a RFD and RFW format based on the requirements in [ACMP 2009, 2017].			
SOW	[SOW-853]	The Contractor SHALL be aware that permanent departures from a baseline SHALL be accomplished by ECP action rather than by RFD/RFW.			
SOW	[SOW-854]	The Contractor SHALL be fully responsible for the CSA for all CIs in accordance with [ACMP 2009, 2017].			
SOW	[SOW-855]	Contractor SHALL prepare and deliver the CSA reports for each milestone and as requested by the Purchaser.			
SOW	[SOW-856]	The Contractor SHALL propose the format of the CSA report in the CM Plan for Purchaser's approval.			
SOW	[SOW-857]	The Contractor SHALL deliver CSA reports to the Purchaser both as part of management and specialist products in this contract and also as standalone documents at the Purchaser's request.			
SOW	[SOW-858]	At the end of the Contract, the Contractor SHALL deliver a set of final CSA reports for each CI or set of CI's in both hard copy and in electronic media.			
SOW	[SOW-859]	Upon request from the Purchaser, the Contractor SHALL support configuration audits to demonstrate that the actual status of all CIs matches the authorised state of CIs as registered in the CSA reports according to [ACMP 2009, 2017].			
SOW	[SOW-860]	The Contractor SHALL support the FCA and PCA by providing the required Baseline Documentation and answering questions from the Purchaser's Auditor.			
SOW	[SOW-861]	The Contractor SHALL draft a Configuration Audit Report for the FCA and PCA that summarises the results for the Purchaser's approval.			
SOW	[SOW-862]	The Contractor SHALL solve any deficiencies found during the Configuration Management Audits within the agreed timeframe and update the baseline accordingly.			

SOW	[SOW-863]	The Contractor SHALL provide the initial version of his ABL and PBL to the Purchaser for acceptance.			
SOW	[SOW-864]	The Contractor SHALL keep the contents of the ABL and PBL under Configuration Control to reflect the progress of the project activities.			
SOW	[SOW-865]	The Contractor SHALL create and maintain a CMDB that persists the CIs attributes, (inter-) relationships, and Configuration Baselines.			
SOW	[SOW-866]	The Contractor SHALL create or use a COTS software to maintain the CMDB that persists the Configuration Items (CIs) attributes, (inter-) relationships and Configuration Baselines.			
SOW	[SOW-867]	The Contractor SHALL ensure that the Configuration Baselines and CIs are persistently stored, maintained and managed in the CMDB.			
SOW	[SOW-868]	The Contractor SHALL keep the CMDB consistent and updated. The Contractor SHALL keep the CMDB consistent and updated.			
SOW	[SOW-869]	The Contractor, through the CMDB, SHALL provide the ability to easily trace higher and subordinate CIs using CI identifiers or other CI attributes.			
SOW	[SOW-870]	The Contractor’s CMDB SHALL be compliant with the Purchaser's IT Service Management (ITSM) Tools.			
SOW	[SOW-871]	The Contractor SHALL use a software source code version control program for any custom software development.			
SOW	[SOW-872]	Subject to approval of the Purchaser under the Technology Substitution clause, the Contractor SHALL establish and maintain the baselines referred to above using the latest commercial version of the version control/Configuration Management automated tool.			
SOW	[SOW-873]	The Contractor, through his provided version control/Configuration Management automated tool, SHALL include the capabilities for baselines management, source control versioning, configuration item identification, change request management, deficiency reporting management, and configuration status accounting.			
SOW	[SOW-874]	The Contractor SHALL provide the Purchaser read-only access to the version control/Configuration Management automated tool.			
SOW	[SOW-875]	The Contractor SHALL provide the ability for the Purchaser to access (read-only) the source code of the baseline via the version control/Configuration Management automated tool.			
SOW	[SOW-876]	The Contractor SHALL provide the version control/Configuration Management automated tool as part of the IEG-C Reference System to enable life-cycle Configuration Management.			
SOW	[SOW-877]	At the end of the contract, the Contractor SHALL transfer the current CMDB database to the Purchaser.			
SOW	[SOW-878]	The Contractor SHALL establish a Configuration Identification System.			
SOW	[SOW-879]	The Contractor’s, through his Configuration Identification System, SHALL identify all documents necessary to provide a full technical description of the characteristics of the Hardware and Software CIs that require control at the time each baseline is established.			
SOW	[SOW-880]	The Contractor, through his Configuration Identification System, SHALL include the relevant deliverables in the contract.			
SOW	[SOW-881]	The Contractor SHALL provide a CI structure in a tree structure with the PBL being the top level CI.			
SOW	[SOW-882]	The Contractor SHALL include detailed proposals for the documents that will comprise the above baselines in the CM Plan for approval by the Purchaser.			
SOW	[SOW-883]	At the end of the contract, the Contractor SHALL deliver the baseline documentation in a format which complies with SOW 11.6.12.			
SOW	[SOW-884]	As part of the CMDB, as specified under Configuration Management Tools, the Contractor SHALL transfer a copy of the current version of all baselines to the Purchaser at contract completion.			
SOW	[SOW-885]	The Contractor SHALL propose the documentation identification and version control system right after the Kick-off Meeting, before the release of the project documentation, for Purchaser approval. The identification SHALL include the project number, the document name and the version of the document. The versioning of the documentation SHALL be applied in a manner that major versions will be applied before each milestone or official delivery, and minor versions will be applied within the review cycles.			
SOW	[SOW-886]	All Contractor's IEG-C project key personnel SHALL demonstrate spoken and written fluency in English language, at a minimum of 4343 as defined in [STANAG 6001, 2014].			
SOW	[SOW-887]	All Contractor's IEG-C project key personnel SHALL have a current NS security clearance and maintain it throughout the lifecycle of the Contract. Contractor personnel who need System Administrator or Operator privileges when working on NATO SECRET systems SHALL be required to hold NATO CTS (Cosmic Top Secret) clearances.			
SOW	[SOW-888]	All Contractor's IEG-C project key personnel SHALL present references of successful project delivery and description of roles, responsibilities, activities executed, and SHALL include reachable points of contact for above.			
SOW	[SOW-889]	The Contractor SHALL assist the Purchaser to configure existing Management Suites in Purchaser’s toolset to integrate and manage IEG-C components, in consistence with the IEG-C system design and management.			

SOW	[SOW-890]	The Contractor SHALL assist the Purchaser to integrate the IEG-C system in the Purchaser's NATO Cyber Security Monitoring Capability.			
SOW	[SOW-891]	The Contractor SHALL provide the Risk Log listing the risks, and indicating for each one the following information (but not limited to): o Risk identifier: unique code to allow grouping of all information on this risk; o Description: brief description of the risk; o Risk category (e.g., management, technical, schedule, and cost risks); o Impact: effect on the project if this risk were to occur; o Probability: estimate of the likelihood of the risk occurring; o Risk rating (High, Medium, Low); o Proximity: how close in time is the risk likely to occur; o Response strategy: avoidance, mitigation, acceptance, transference o Response plan(s): what actions have been taken/will be taken to counter this risk; o Owner: who has been appointed to keep an eye on this risk; o Author: who submitted the risk; o Date identified: when was the risk first identified; o Date of last update: when was the status of this risk last checked; o Status: e.g., closed, reducing, increasing, no change.			
SOW	[SOW-892]	The Contractor SHALL ensure that the Issue Log comprises the following information (but not limited to): o Project Issue Number; o Project Issue Type (ECP, Off-specification, general issue such as a question or a statement of concern); o Author; o Date identified; o Date of last update; o Description; o Action item; o Responsible person. (Individual in charge of the action item); o Suspense date (Suspense date for the action item); o Priority; o Status.			
SOW	[SOW-893]	The Contractor SHALL ensure that the PSR summarises activities and progress, including (but not limited to): o Changes in key Contractor personnel; o Summary of Contract activities during the preceding month, including the status of current and pending activities; o Progress of work and schedule status, highlighting any changes since the preceding report; o EVM KPIs, including Planned Value, Earned Value, Actual Cost, Schedule Variance, Schedule Performance Index, Budget at Completion and Estimate at Completion. o CSA report addressing all products in the Project Breakdown Structure; o Issue Log; o Change Requests status; o Off-Specifications status; o Risk Log; o Test(s) conducted and results; o Summary of any site surveys conducted; o Plans for activities during the following reporting period; o Provisional financial status and predicted expenditures.			
SOW	[SOW-894]	The Contractor SHALL ensure that any Change Request will respect the requirements in SOW 12.7 Requests for Change (RFC).			

SOW	[SOW-895]	The Contractor SHALL ensure that CR documentation includes: o The list of all Change Requests processed since the start of the project, in a tabular form, indicating for each of them the date it was created and the current status; o All Change Requests processed since the start of the project.			
SOW	[SOW-896]	The Contractor SHALL include, at a minimum, the following information in the SDS document: o System Architecture o The following Operational and Systems Views, as defined in the NATO Architecture Framework (NAF, [NAC AC/322-D(2007)0048, 2007]): o NOV-1, High-Level Operational Concept Diagram; o NSV-1 Systems Interface Description (Composition); o NSV-1 System Interface Description (Intra System); o NSV-1 System Interface Description (Inter System); o NSV-2a: System Port Specification; o NSV-4 System Functionality;			
SOW	[SOW-897]	The (minimum) information in the NAF views the Contractor SHALL supply is defined in Table 26 below: NSV-1 (composition) NSV-1 (intra-system) NSV-1 (inter-system) NSV-1 (deployment) NSV-2a (System port description) aka Interface Specification NSV-4 (system functionality)			
SOW	[SOW-898]	The NAF views SHALL be produced using applications compliant with NAF 4 and Archimate 3. If not, the Contractor SHALL ensure the exchange format SHALL be approved by the Purchaser upfront.			

SOW	[SOW-899]	Physical layout and operation principles of the IEG-C in the deployment sites (including the site of the IEG-C Reference System): identification of where the components will be installed, of how users (NATO Staff Users) will make use of the provided functionality, of how support staff (IEG-C Administrators will operate the system. This SHALL cover in particular how the IEG-C components SHALL integrate into the storage and backup solutions existing at the implementation sites. o Results of the network simulation, showing the integration with the underlying network infrastructure, the mitigation of potential impact of the available bandwidth and of any latency; o Replication, synchronisation and browsing protocols and flows; o Proposed topology for the system; o Routing, Transport, and connectivity to IEG-C components; o Administration model design (Administrative groups and permissions, administrative roles, trust relationships between separate domains). o Schema o Attributes to which the NATO Staff Users have read-access. o System Functionalities. o Functional breakdown of the IEG-C system. o Application Programming Interfaces (API) and libraries. o System internal interfaces: Description of the interworking of all components to meet the system requirements (e.g., physical interfaces between components, data flows.) o Performance Requirements: Performance requirements are defined in the SRS. o Equipment o Physical breakdown of the operational IEG-C system, of the Reference Test Bed, into hardware/software CIs (including the number of licenses for each software CI), with traceability to the functional breakdown. o Identification of all COTS included in the system. o CSA reports addressing all system CIs. o All configuration information (parameters, settings, etc.) for all of the IEG-C components. o Security o Description of how the system complies with all security requirements.			
SOW	[SOW-900]	The SVDD SHALL include the following: o List of differences between this and the previous System version; o List of capabilities of this System version; o Guidelines on how to install this System version; o Breakdown of the system into CIs and provision of accurate identification information for every CI.			
SOW	[SOW-901]	The Contractor SHALL submit to the Purchaser the SIP with the following information: o The Contractor's approach to all system implementation tasks (including the sequence of activation of the sites to be implemented); o The Contractor organisation and key personnel involved in system implementation; o The overall schedule for implementation activities including site survey, site preparation, site installation and activation. This schedule SHALL show all planned outages of any kind in the sites; o The schedule of all planned outages of any kind in the sites;			
SOW	[SOW-902]	The detailed implementation sequence of Technical Services and User services. The sequence SHALL carefully consider and adapt to the ITM implementation sequence in order to minimize the impacts on both projects.			

SOW	[SOW-903]	The installation plan, which SHALL specifically address: o A general installation plan showing how the gradual installation and activation of the IEG-C will be carried out by the Contractor; o The installation procedures, showing that those procedures will cause no or minimal disruption to the sites and to the User desktop applications; o A site-specific design for each site; o A detailed installation plan for each site; o Site and system installation checklist; o Site activation checklist; o An Allocation Matrix showing the allocation of each system CIs (nature and quantities) to each site, and the number of users and support staff for each site; o Any specific tools the Contractor intends to furnish and use during the site installation.			
SOW	[SOW-904]	The activation plan, which SHALL specifically address: o The site activation activities; o Any post-activation tasks; o The "back-out" procedures. The back-out section to the SIP SHALL enable deactivation and/or removal of all installed IEG-C components and restoration of existing services without disruption of those services. o The potential disruption/outage that the implementation activities might generate ensuring potential outages will be kept short (less than 3 hours in duration), planned (approved by the Purchaser at 48 hours in advance based on a Contractor-provided plan to restore functionality within 30 minutes), localised (limited to areas agreed to by the Purchaser), and if possible carried out during week-ends. o The migration plan from existing gateways to IEG-C:			
SOW	[SOW-905]	The migration plan SHALL detail the migration activities. Schedule. Engineering activities for the migration of the existing gateways to IEG-C.			
SOW	[SOW-906]	The Contractor SHALL structure the SIP so that general implementation information is maintained in the body of the plan and site-specific details are kept as annexes.			
SOW	[SOW-907]	The Contractor SHALL ensure that the PMP comprises at minimum of the following sections: o An ‘Organisation’ section describing the Contractor’s organisation for this project according to the requirements. This section SHALL include an organisational chart showing the members of the Contractor’s Project Team (including the members of the Contractor PMO) and showing their respective responsibilities and authority. This section should also include proposed Project Communication Plan. o A ‘Project Planning’ section describing the Contractor’s processes supporting the development and maintenance of the PBS, PFD and PMS according to the requirements. o A ‘Risk management’ section describing the Contractor’s processes supporting Risk Management by the Contractor. o A ‘System Engineering’ section describing the Contractor approach to these activities according to the requirements in SECTION 10. o A ‘System Implementation’ section describing the Contractor approach to these activities according to the requirements in SECTION 13. o An ‘Operation and Maintenance’ section describing the Contractor approach to these activities according to the requirements in SECTION 12. o An "Operation and Maintenance" section describing the Contractor approach to these activities according to the requirements in Annex F: Annex F Maintenance and Support Concept (After FSA); o A ‘Testing’ section describing the Contractor approach to these activities according to the requirements in SECTION 14. o An “Earned Value Management Section” describing how the Contractor will assure EVM tracking and reporting			
SOW	[SOW-908]	The Contractor SHALL develop all Technical Manuals compliant with the requirements in SOW 11.6.			
SOW	[SOW-909]	The Contractor SHALL develop Standard Operating Procedures which detail the supporting processes described in ANNEX F.			

SOW	[SOW-910]	The Contractor SHALL be prepared to procure all hardware required for the completion of this project, if the Purchaser exercises the corresponding option before the PDR (EDC+3MO).			

Reference Document	Reference ID *(BI, SOW requirement, SRS requirement)*	Description	Bid Reference	Remarks	Compliance statement
SOW Annex-A	[SRS-3-1]	The IEG-C SHALL provide a data exchange capability IEG-C_DEX that facilitates the mediation of data between the High Domain and the Low Domain.			
SOW Annex-A	[SRS-3-10]	The Intrusion Detection Services SHALL offer the following functionality to provide protection for the integrity of the NATO Secret network and protection for availability of the NATO Secret network: • Detect Malicious Activities and Faults; • Prevent and mitigate Attacks and Fault			
SOW Annex-A	[SRS-3-101]	All IEG-C components SHALL support 1GbE.			
SOW Annex-A	[SRS-3-102]	All IEG-C components SHALL be upgradeable, through the use of pluggable transceivers, to support 10GbE.			
SOW Annex-A	[SRS-3-11]	The Public Key Cryptographic Services SHALL offer the following functionality to provide protection for the confidentiality of the NATO Secret network and protection for the integrity of the NATO Secret network: • Process Public Key Cryptographic Data • Manage Cryptographic Keys			
SOW Annex-A	[SRS-3-12]	The Content Inspection Services SHALL offer the following functionality to provide protection for the confidentiality, integrity and availability of the NATO Secret network: • Identify Content; • Verify Content; and, • Transform Content.			
SOW Annex-A	[SRS-3-13]	The Protection Policy Enforcement Services SHALL enforce protection policies on mediated data.			
SOW Annex-A	[SRS-3-14]	The Protection Policy Enforcement Services SHALL consider all aspects relevant to protection of confidentiality, integrity and availability. The Protection Policy Enforcement Services consists of the following two services: • Information Flow Control Policy Enforcement (IFCPE) Services; and, • Content Inspection Policy Enforcement (CIPE) Services.			
SOW Annex-A	[SRS-3-15]	The IFCPE Services SHALL enforce Information flow policies (IFP), which constitute a subset of protection policies.			
SOW Annex-A	[SRS-3-16]	The IFPs SHALL define the way information moves between the NATO Secret network and the Mission Secret network, and vice-versa based upon the following criteria: • the subjects (for example, this may be the IP address of the source and destination, or originator and recipient domain for email or text-based collaboration chat, or the source and destination interfaces within the IEG-C where the IFP is being enforced) under control of the policy; • the content (the data type i.e. XML, that is being exchanged by the Data Exchange Service supporting the information exchange requirement) under control of the policy; and • the operations which cause information to flow to and from controlled subjects covered by the policy.			
SOW Annex-A	[SRS-3-17]	The Information Flow Control Policy Enforcement (IFCPE) Services SHALL enforce the following general IFPs: • IEG-C_IFP_CA_HL - Communications Access Services High to Low IFP; • IEG-C_IFP_CA_LH - Communications Access Services Low to High IFP; • IEG-C_IFP_IS_HL - Infrastructure Services High to Low IFP; • IEG-C_IFP_SOA_HL - SOA Platform Services High to Low IFP; • IEG-C_IFP_SOA_LH - SOA Platform Services Low to High IFP; • IEG-C_IFP_BS_HL - Business Support Services High to Low IFP; • IEG-C_IFP_BS_LH - Business Support Services Low to High IFP; and, • IEG-C_IFP_CS_MGMT - Core Services Management Services IFP.			
SOW Annex-A	[SRS-3-18]	The Content Inspection Policy Enforcement (CIPE) Services SHALL enforce Content Inspection Policies (CIPs) which define how the data mediated between the NATO Secret network and NATO-led Mission network is to be inspected.			
SOW Annex-A	[SRS-3-19]	The CIPs SHALL be designed to protect the confidentiality of the NATO Secret network by inspecting data for unauthorised information that should not be released to the NATO-led Mission Network.			
SOW Annex-A	[SRS-3-2]	IEG-C_DEX SHALL offer the physical network interface IEG-C High Domain Interface [NCIA TR/2016/NSE010871/01, 2017] (IEG-C_IF_NET_HIGH) that provides Ethernet connectivity to the High Domain.			
SOW Annex-A	[SRS-3-20]	The CIPs SHALL be designed to protect the integrity and availability of the NATO Secret network by identifying and verifying the structure of the data and removing or blocking malicious content.			
SOW Annex-A	[SRS-3-21]	CIPE Services SHALL enforce the following general CIPs: • IEG-C_CIP_SOA_HL - SOA Platform Services High to Low CIP; • IEG-C_CIP_SOA_LH - SOA Platform Services Low to High CIP; • IEG-C_CIP_BS_HL - Business Support Services High to Low CIP; • IEG-C_CIP_BS_LH - Business Support Services Low to High CIP; • IEG-C_CIP_COI-ES_HL - COI-Enabling Services High to Low CIP; • IEG-C_CIP_COI-ES_LH - COI-Enabling Services Low to High CIP; • IEG-C_CIP_COI_HL - COI-Specific Services High to Low CIP; and • IEG-C_CIP_COI_LH - COI-Specific Services Low to High CIP.			
SOW Annex-A	[SRS-3-22]	The IEG-C Element Management Services SHALL provide interfaces that can be managed from a centralized management system to support activities such as Service Management and Control (SMC), Cyber-Defence, security policy administration, audit management and IEG-C configuration and maintenance.			
SOW Annex-A	[SRS-3-23]	The Element Management Services SHALL support the different administrative roles that are required for managing the IEG-C.			
SOW Annex-A	[SRS-3-24]	The administrative roles of the IEG-C SHALL be categorised as follows: • System Administrator: responsible for installation, configuration and maintenance of the IEG-C; • Local System Administrator: responsible for installation, configuration and maintenance of a subset of IEG-C's; • Local System Maintainer: responsible for some maintenance activities of a subset of IEG-C's; • Audit Administrator: responsible for regular review of IEG-C audit logs; • CIS Security Administrator: responsible for performing the IEG-C CIS security-related tasks, such as security policy management; • Cyber Defence Administrator: responsible for monitoring and performing cyber-related tasks; and, • SMC Administrator: responsible for monitoring IEG-C services. • Local SMC Administrator: responsible for monitoring a subset of IEG-C's services and components.			
SOW Annex-A	[SRS-3-25]	The IEG-C Element Management Services SHALL provide interfaces to support local management activities such as Service Management and Control (SMC), Cyber-Defence, security policy administration, audit management and IEG-C configuration and maintenance, in case of loss of connectivity with the Central Management system.			
SOW Annex-A	[SRS-3-3]	IEG-C_DEX SHALL offer the physical network interfaces IEG-C Low Domain Interfaces [NCIA TR/2016/NSE010871/01, 2017] (IEG-C_IF_NET_LOW) that provides Ethernet connectivity to the Low Domains.			
SOW Annex-A	[SRS-3-4]	IEG-C_DEX MAY offer the physical network interface IEG-C Management Interface [NCIA TR/2016/NSE010871/01, 2017] (IEG-C_IF_MGMT) that provides Ethernet connectivity to the High Domain.			
SOW Annex-A	[SRS-3-5]	In the case that IEG-C_DEX cannot offer the physical network interface IEG-C_IF_MGMT, it SHALL offer a logical network interface IEG-C_IF_MGMT on top of IEG-C_IF_NET_HIGH.			
SOW Annex-A	[SRS-3-6]	The IEG-C SHALL offer the following functionality as described in the IEG-C Architecture Building Blocks [NCIA TR/2016/NSE010871/01, 2017]: • Provide CIS connectivity; • Create Network Boundary; • Create Domain Boundary; • Protect Confidentiality of High Domain; • Protect Integrity of High Domain; • Protect Availability of High Domain; • Mediate Data Exchange; and, • Centralize Management.			
SOW Annex-A	[SRS-3-7]	The design and architecture of the IEG-C for providing protected cross domain information exchange between NATO Secret and NATO-led Mission Secret SHALL be implemented in accordance with the self-protecting node principle [NAC AC/35-D/2004-REV3, 2013].			
SOW Annex-A	[SRS-3-8]	The Data Exchange Services SHALL offer the following functionality to provide CIS Interconnectivity and Mediate Data Exchange: • Exchange Email Services Data; • Exchange Web Services Data; • Provide Remote Desktop Access; • Exchange Network Services Data; and, • Exchange Text Based Collaboration Services Data			
SOW Annex-A	[SRS-3-9]	The Protection Services SHALL provide the capability to protect data at the network layer and the application layer. The Protection Services consists of the following three atomic services: • Intrusion Detection Services; • Public Key Cryptographic Services; and, • Content Inspection Services.			

SOW Annex-A	[SRS-4-1]	The IEG-C (depending upon the IERs and protection policies to be enforced for the CIS interconnection) SHALL consist of the following components: • Firewalls; • Network Switches; • RDP Proxy; • Web Proxy; • Mail Guard; and, • Web Guard.			
SOW Annex-A	[SRS-4-10]	IEG-C_DEX SHALL offer Simple Mail Transfer Protocol (SMTP) [IETF RFC 5321, 2008] interface 'Business Support Services HL' on top of 'Communications Access Services HL' and Simple Mail Transfer Protocol (SMTP) [IETF RFC 5321, 2008] interface 'Business Support Services LH' on top of 'Communications Access Services LH'.			
SOW Annex-A	[SRS-4-100]	The IEG-C Web Proxy component SHALL be enabled and configured with the capability for being managed as specified in Section 9.			
SOW Annex-A	[SRS-4-101]	The TLS Server identity (X.509 PKIX version 3.0 certificate, [IETF RFC 5280, 2008]) SHALL be validated, as per Section 6 of [IETF RFC 6125, 2011] following the best current practices documented in the "Recommendations for Secure Use of TLS and DTLS" [IETF RFC 7525, 2015(IETF)].			
SOW Annex-A	[SRS-4-101]	The IEG-C Web Proxy component SHALL be an appliance, or deployed on a physical server.			
SOW Annex-A	[SRS-4-102]	IEG-C_DEX SHALL offer an interface "Core Services" on top of 'Communications Access Services Management' that SHALL support the following protocols: • DNS [IETF RFC 1035, 1987] • OCSP [IETF RFC 6960, 2013] • LDAP [IETF RFC 4510-4519, 2006] • RTP [IETF RFC 3350, 2003] • RTCP [IETF RFC 3350, 2003] • JREAP [STANAG 5518]			
SOW Annex-A	[SRS-4-103]	The IEG-C Web Proxy component SHALL be configured to have at least three network interfaces (NICs: one for the network connection to the High Domain Switch; one for the network connection to the Low Domain Switches; and, one for the network connection to the Management Domain Switch).			
SOW Annex-A	[SRS-4-105]	The IEG-C RDP Proxy component SHALL be the Microsoft Windows Server 2016 (or later versions that are listed on the Approved Fielded Product List for the High Side) with the Remote Desktop Services server role.			
SOW Annex-A	[SRS-4-106]	The IEG-C RDP Proxy component SHALL be synchronised to the IEG-C High Domain Firewall component NTP source.			
SOW Annex-A	[SRS-4-106]	Local client devices SHALL NOT be accessible on the remote desktop session.			
SOW Annex-A	[SRS-4-107]	The IEG-C RDP Proxy component SHALL enable the capability to support only those Data Exchange Services as specified in Table 4 (for that component).			
SOW Annex-A	[SRS-4-107]	The IEG-C RDP Proxy component SHALL be enabled and configured with the capability for being managed as specified in Section 9.			
SOW Annex-A	[SRS-4-108]	The IEG-C RDP Proxy component SHALL generate an SSL Certificate Signing Request (CSR) to be signed by the appropriate E-NPKI Registration Authority (RA).			
SOW Annex-A	[SRS-4-109]	The IEG-C RDP Proxy component SHALL be deployed on a physical server.			
SOW Annex-A	[SRS-4-11]	IEG-C_DEX SHALL offer Remote Desktop Protocol (RDP) [RDP Overview, 2019] interface 'Infrastructure Services HL' on top of 'Communications Access Services HL'.			
SOW Annex-A	[SRS-4-110]	The IEG-C RDP Proxy component server SHALL support (as a minimum) the Microsoft Windows Server 2016 R2 (or later versions that are listed on the Approved Fielded Product List for the High Side) 64-bit edition operating system.			
SOW Annex-A	[SRS-4-111]	The IEG-C RDP Proxy component server SHALL be configured to have at least three network interfaces (NICs: one for the network connection to the High Domain Switch; one for the network connections to the Low Domain Switch; and, one for the network connection to the Management Domain Switch).			
SOW Annex-A	[SRS-4-113]	The IEG-C Web Guard component SHALL comply with the functional requirements specified in Section 6.			
SOW Annex-A	[SRS-4-114]	The IEG-C Web Guard component SHALL comply with the non-functional requirements specified in Section 5.3.			
SOW Annex-A	[SRS-4-115]	The IEG-C Web Guard component SHALL comply with the security functional requirements specified in Section 6.8.			
SOW Annex-A	[SRS-4-116]	The IEG-C Web Guard component SHALL be synchronised to the IEG-C High Domain Firewall component NTP source.			
SOW Annex-A	[SRS-4-118]	It SHALL be possible to enforce a separate 'WG security policy' (see section 6.2.1) per service/application mediated by the Web Guard.			
SOW Annex-A	[SRS-4-119]	The IEG-C Web Guard component SHALL enable the capability to support only those Data Exchange Services as listed in Table 4 (for that component) and specified in Section 6.4.			
SOW Annex-A	[SRS-4-12]	IEG-C_DEX SHALL offer UDP [IETF RFC 768, 1980] and IPv4 and IPv6, [IETF RFC 791, 1981], [IETF RFC 8200, 2017] over Ethernet interface 'Communications Access Services Management' on top of IEG-C_IF_MGMT.			
SOW Annex-A	[SRS-4-120]	The IEG-C Web Guard component Protection Services SHALL comply with the requirements specified in Section 6.6.			
SOW Annex-A	[SRS-4-121]	The IEG-C Web Guard component Protection Policy Enforcement Services SHALL comply with the requirements specified in Section 6.5.			
SOW Annex-A	[SRS-4-122]	The IEG-C Web Guard component Element Management Services SHALL comply with the requirements specified in Section 6.7.			
SOW Annex-A	[SRS-4-123]	The IEG-C Web Guard component SHALL be configured to have at least three network interfaces (NICs: one for the network connection to the High Domain Switch; one for the network connection to the Low Domain Switch; and, one for the network connection to the Management Domain Switch).			
SOW Annex-A	[SRS-4-124]	The IEG-C Web Guard component network interfaces to the High Domain Switch, Low Domain Switches and Management Domain Switch SHALL be 1000BASE-SX gigabit Ethernet interfaces.			
SOW Annex-A	[SRS-4-126]	The IEG-C Mail Guard component SHALL be synchronised to the IEG-C Firewall component NTP source.			
SOW Annex-A	[SRS-4-127]	The IEG-C Mail Guard component SHALL enable the capability to support only those Data Exchange Services as specified in Table 4 (for that component).			
SOW Annex-A	[SRS-4-128]	The IEG-C Mail Guard component SHALL use a malware/virus scanner that is included in the NATO Information Assurance Product Catalogue (NIAPC) to check email messages for malicious content.			
SOW Annex-A	[SRS-4-129]	The IEG-C Mail Guard component SHALL enable the capability to configure the Content Inspection Services that will enforce the IEG-C Business Support and COI CIPs (refer to Section 4.7.4) depending on the information exchange requirements and the content inspection policy to be enforced for the CIS interconnection.			
SOW Annex-A	[SRS-4-13]	IEG-C_DEX SHALL offer an interface 'Core Services Management' on top of 'Communications Access Services Management' that SHALL support the following management protocols: • Keyboard, video and mouse (KVM) over Internet Protocol (IP); • Command Line interface (CLI) via Secure Shell (SSH) Transport Layer protocol [IETF RFC 4251, 2006]; • Simple Network Management Protocol (SNMP) Version 3 [IETF RFC 3410 – 3418, 2002]; • Syslog [IETF RFC 5424, 2009]; • Secure Shell (SSH, [IETF RFC 4253, 2006]); • Network Time Protocol (NTP, [IETF RFC 5905, 2010]); • Intelligent Platform Management Interface (IPMI, [IPMI V.2.0, 2013]); • Hyper-Text Transport Protocol (HTTP) v1.1 Web interface [IETF RFC 7230, 2014] [IETF RFC 7231, 2014] • Hyper-Text Transport Protocol (HTTP) v2 Web interface [IETF RFC 7540, 2014] ; • Remote Desktop (RDP [RDP Overview, 2019]; • Remote Procedure Call (RPC, [IETF RFC 5531, 2009]). • System Center Operations Manager • Systems Center Configuration Manager • Windows Server Update Services • McAfee e-Policy Orchestrator • Adobe Patching • File Transfer Protocol [IETF RFC 959, 1985] • Telnet [IETF RFC 854, 1983]			
SOW Annex-A	[SRS-4-130]	The IEG-C Mail Guard component SHALL enable the capability to perform cryptographic operations and key management to support the validation of cryptographic bindings according to NISP Cryptographic Artefact Binding Profiles [ADatP-34(I), NISP Version 10, 2017].			
SOW Annex-A	[SRS-4-131]	The IEG-C Mail Guard component SHALL be configured to conform to the INFOSEC CIS Security Technical and Implementation Guidance in Support of Public Key Infrastructure - Cryptographic Aspects [NAC AC/322-D(2007)0002-REV1, 2015].			
SOW Annex-A	[SRS-4-132]	The IEG-C Mail Guard component SHALL be configured to conform to the INFOSEC Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanisms [NAC AC/322-D/0047-REV2 (INV), 2009].			
SOW Annex-A	[SRS-4-133]	The IEG-C Mail Guard component provided cryptographic mechanism SHALL be configured based on Technical Implementation Guidance on Cryptographic Mechanisms in Support of Cryptographic Services [NAC AC/322-D(2012)0022, 2013].			
SOW Annex-A	[SRS-4-134]	The IEG-C Mail Guard component SHALL be configurable to support the enforcement of the following IEG-C Business Support IFPs (see Section 3.4.4):			
SOW Annex-A	[SRS-4-135]	The IEG-C Mail Guard component SHALL be configurable to support the enforcement of the following IEG-C Business Support CIPs (see Section 3.4.5):			
SOW Annex-A	[SRS-4-136]	The IEG-C Mail Guard component SHALL enable the capability to configure the MG_IFP_BS_HL IFP in order to guard SMTP application-level traffic from the high domain to the low domain.			
SOW Annex-A	[SRS-4-137]	The IEG-C Mail Guard component SHALL enable the capability to configure the MG_IFP_BS_LH IFP in order to guard SMTP application-level traffic from the low domain to the high domain.			

SOW Annex-A	[SRS-4-138]	The IEG-C Mail Guard component SHALL enable the capability to configure the MG_IFP_BS_HL and MG_IFP_BS_LH IFPs to verify that the email message can be forwarded between the high and low domain by checking originator access control rules against white or black lists.			
SOW Annex-A	[SRS-4-139]	The IEG-C Mail Guard component SHALL enable the capability to configure the MG_IFP_BS_HL and MG_IFP_BS_LH IFPs to verify that the email message can be transferred between the high and low domain by checking recipient access control rules against white or black lists.			
SOW Annex-A	[SRS-4-14]	Installation guidelines for "Selection and Installation of Equipment for the Processing of Classified Information" [SDIP-29/2] regarding equipment separation and installation requirements SHALL be adhered to.			
SOW Annex-A	[SRS-4-140]	The IEG-C Mail Guard component SHALL enable the capability to configure the MG_IFP_BS_HL IFP to enforce the MG_CIP_BS_HL CIP.			
SOW Annex-A	[SRS-4-141]	The IEG-C Mail Guard component SHALL enable the capability to configure the MG_CIP_BS_HL CIP to verify that all email messages to be released from the high domain to the low domain contain a security label that conforms to the access control rules to be enforced for the CIS interconnection.			
SOW Annex-A	[SRS-4-142]	The IEG-C Mail Guard component SHALL enable the capability to select that the security label format is the STANAG 4774 confidentiality label XML format.			
SOW Annex-A	[SRS-4-143]	The IEG-C Mail Guard component SHALL enable the capability to select that the STANAG 4774 confidentiality label is bound to the email message as specified in STANAG 4778 and NATO Interoperability Standards and Profiles (NISP) SMTP Binding Profile.			
SOW Annex-A	[SRS-4-144]	The IEG-C Mail Guard component SHALL enable the capability to select that the STANAG 4774 confidentiality label is cryptographically bound to the email message as specified in NATO Interoperability Standards and Profiles (NISP) Cryptographic Artefact Binding Profiles.			
SOW Annex-A	[SRS-4-145]	~~The IEG-C Mail Guard component SHALL enable the capability to configure the MG_CIP_BS_HL CIP to verify that all email messages to be released from the high domain to the low domain do not contain unauthorised information, such as 'dirty words'~~.			
SOW Annex-A	[SRS-4-146]	The IEG-C Mail Guard component SHALL enable the capability to configure the MG_IFP_BS_LH IFP to enforce the MG_CIP_BS_LH CIP.			
SOW Annex-A	[SRS-4-147]	The IEG-C Mail Guard component SHALL enable the capability to configure the MG_CIP_BS_HL and MG_CIP_BS_HL CIPs to verify that all email messages to be forwarded between the high domain and the low domain do not contain any disallowed attachment types by checking against a white list or black list of attachment types.			
SOW Annex-A	[SRS-4-148]	The IEG-C Mail Guard component SHALL enable the capability to configure the MG_CIP_BS_LH CIP to verify that all email messages (including email message header, body and allowed body parts) are well-formed, valid and contain no malicious content.			
SOW Annex-A	[SRS-4-149]	Depending on the information exchange requirements the IEG-C SHALL be configurable to support the enforcement of the following IEG-C COI CIPs (see Section 3.4.5): • IEG-C_CIP_COI-ES_HL - COI-Enabling Services High to Low CIP; • IEG-C_CIP_COI-ES_LH - COI-Enabling Services Low to High CIP; • IEG-C_CIP_COI_HL - COI-Specific Services High to Low CIP; and • IEG-C_CIP_COI_LH - COI-Specific Services Low to High CIP.			
SOW Annex-A	[SRS-4-15]	The IEG-C SHALL support a network architecture containing a de-militarized zone (DMZ).			
SOW Annex-A	[SRS-4-150]	The IEG-C Mail Guard component SHALL enable the capability to configure the IEG-C_CIP_COI-ES_HL and IEG-C_CIP_COI_HL CIPs to verify that attachments contained in email messages to be released from the high domain to the low domain do not contain unauthorised information, such as 'dirty words', including classification markings.			
SOW Annex-A	[SRS-4-151]	The IEG-C Mail Guard component SHALL enable the capability to configure the IEG-C_CIP_COI-ES_LH and IEG-C_CIP_COI_LH CIPs to verify that attachments contained in email messages are well-formed, valid and contain no malicious content.			
SOW Annex-A	[SRS-4-152]	The IEG-C Mail Guard component SHALL enforce the IEG-C Business Support IFPs, Business Support CIPs and COI CIPs configured (depending upon the information exchange requirements and protection policy enforced for the CIS interconnection) for the IEG-C.			
SOW Annex-A	[SRS-4-153]	The IEG-C Mail Guard component SHALL be enabled and configured with the capability for being managed as specified in Section 9.			
SOW Annex-A	[SRS-4-154]	The IEG-C Mail Guard component SHALL be configured to have at least three network interfaces (NICs: one for the network connection to the High Domain Switch; one for the network connections to the Low Domain Switch; and, one for the network connection to the Management Domain Switch).			
SOW Annex-A	[SRS-4-155]	The IEG-C Mail Guard component network interfaces to the High Domain Switch, Low Domain Switches and Management Domain Switch SHALL be 1000BASE-SX gigabit Ethernet interfaces.			
SOW Annex-A	[SRS-4-156]	The IEG-C server SHALL be integrated with either: • HPE OneView and HPE Integrated Lights-Out (iLO); or • Dell EMC OpenManage Enterprise and Dell Integrated Dell Remote Access Controller (iDRAC)			
SOW Annex-A	[SRS-4-158]	The IEG-C server component SHALL be configured to have at least three network interfaces (NICs: one for the network connection to the High Domain Switch; one for the network connections to the Low Domain Switch; and, one for the network connection to the Management Domain Switch).			
SOW Annex-A	[SRS-4-159]	The IEG-C server component network interfaces to the High Domain Switch, Low Domain Switch and Management Domain Switch SHALL be 1000BASE-SX gigabit Ethernet interfaces.			
SOW Annex-A	[SRS-4-160]	The IEG-C server component SHALL be synchronised to the IEG-C High Domain Firewall component NTP source.			
SOW Annex-A	[SRS-4-165]	The IEG-C Rack component SHALL be the Server Equipment Cabinet			
SOW Annex-A	[SRS-4-167]	All IEG-C components SHALL be rack mounted.			
SOW Annex-A	[SRS-4-168]	The IEG-C UPS component SHALL be the UPS APC Smart-UPS C 1500..			
SOW Annex-A	[SRS-4-169]	The IEG-C components providing 1000BASE-SX gigabit Ethernet physical interfaces SHALL be connected with multi-mode fibre optic cables.			
SOW Annex-A	[SRS-4-17]	To support connectivity of the proxies and the guards to the high domain and the low domains the High Network Domain Switch and a Low Domain Network Switch SHALL be provided, respectively.			
SOW Annex-A	[SRS-4-172]	All network interfaces shall be implemented in accordance with [IEEE 802.3:2012], whereby, gigabit Ethernet interfaces shall support a maximum transmission unit (MTU) of 9000 bytes.			
SOW Annex-A	[SRS-4-18]	The High Domain Switch SHALL be connected to the High Domain Firewall.			
SOW Annex-A	[SRS-4-19]	The Low Domain Switch SHALL be connected to the Low Domain Firewall.			
SOW Annex-A	[SRS-4-2]	Only those IEG-C components, hence only the protocols, network services, and the information or data flows, required to support the information exchange requirements SHALL be configured and used through the interconnection.			
SOW Annex-A	[SRS-4-20]	The RDP Proxy SHALL be connected to the High Domain Firewall (via the High Domain Network Switch) and the Low Domain Firewall (via the Low Domain Network Switch) using separate physical network interfaces.			
SOW Annex-A	[SRS-4-200	The IEG-C wired infrastructure for connecting IEG-C components (that are required to be connected together to support the information exchange requirements for the CIS interconnection) SHALL support VLANs.			
SOW Annex-A	[SRS-4-201]	The selected IEG-C High Domain and Low Domain Firewalls components SHALL include compatible rack mount kits and power cords.			
SOW Annex-A	[SRS-4-202]	The IEG-C High Domain Firewall and IEG-C Low Domain Firewall components SHALL mediate all Data Exchange Services that transition the IEG-C.			
SOW Annex-A	[SRS-4-203]	The IEG-C High Domain Firewall and Low Domain Firewall components SHALL enable the capability to configure the IEG-C_IFP_CA_HL and IEG-C_IFP_CA_LH IFPs in order to allow only those application layer protocols and applications that are required to support the information exchange requirements for the high domain - low domain interconnection.			
SOW Annex-A	[SRS-4204]	The IEG-C High Domain Firewall and Low Domain Firewall components SHALL identify application layer protocols and applications through application protocol inspection, which SHALL be based on the use of application signatures, application protocol decoding, and heuristics.			
SOW Annex-A	[SRS-4-205]	The IEG-C High Domain Firewall and Low Domain Firewall components SHALL be managed from the Service Operation Centre (SOC) using the current management tools (i.e. Palo Alto Networks Panorama).			
SOW Annex-A	[SRS-4-206]	The IEG-C Low Domain Firewall component SHALL be configured to have at least three network interfaces (NICs: one for the network connection to the low domain; one for the network connection to the Low Domain Network Switch; and, one for the network connection to the Management Domain Network Switch).			
SOW Annex-A	[SRS-4-207]	The IEG-C Low Domain Firewall component network interfaces to the low domain SHALL be 1000-BaseSX gigabit Ethernet interfaces.			
SOW Annex-A	[SRS-4-208]	The IEG-C Low Domain Firewall component network interfaces to the Low Domain Switch SHALL be 1000BASE-SX gigabit Ethernet interfaces.			
SOW Annex-A	[SRS-4-209]	The selected IEG-C Network Switch components SHALL include compatible rack mount kits and power cords.			
SOW Annex-A	[SRS-4-21]	The Web Proxy SHALL be connected to the High Domain Firewall (via the High Domain Network Switch) and the Low Domain Firewall (via the Low Domain Firewall) using separate physical network interfaces.			
SOW Annex-A	[SRS-4-210]	Only configured users SHALL be allowed to connect to the RDP Proxy.			
SOW Annex-A	[SRS-4-211]	Users SHALL be required to authenticate to the RDP Proxy in accordance with [NAC AC/322-D/0048-REV3, 2019].			
SOW Annex-A	[SRS-4-212]	Authenticated users SHALL be required to authenticate to the RDP Proxy in accordance with [NAC AC/322-D/0048-REV3, 2019].			
SOW Annex-A	[SRS-4-213]	An authenticated user SHALL only be able to connect to a configured set of network resources.			
SOW Annex-A	[SRS-4-214]	The IEG-C management workstation component SHALL be the Dell Optiplex 5070 SFF or equivalent, satisfying the tempest requirements defined at the site survey			
SOW Annex-A	[SRS-4-215]	The IEG-C management workstation monitor SHALL be the Dell P2419H Monitor.			
SOW Annex-A	[SRS-4-216]	The IEG-C management workstation keyboard SHALL be the Dell KB216 Multimedia Keyboard.			
SOW Annex-A	[SRS-4-217]	The IEG-C management workstation mouse SHALL be the Dell 6 Button Laser Mouse.			
SOW Annex-A	[SRS-4-218]	Any IEG-C component MAY host a Type 1 Hypervisor, provided that the overall IEG-C system design meets the requirements of "Technical and Implementation Directive for CIS Security" [NAC AC/322-D/0048-REV3, 2019] (see SRS-4-4).			
SOW Annex-A	[SRS-4-219]	The Type 1 Hypervisor for the server and the management workstation, if used, SHALL be the VMWare ESXi hypervisor.			
SOW Annex-A	[SRS-4-22]	The Mail Guard SHALL be connected to the High Domain Firewall (via the High Domain Network Switch) and the Low Domain Firewall (via the Low Domain Network Switch) using separate physical network interfaces.			

SOW Annex-A	[SRS-4-220]	The IEG-C power distribution component SHALL be the Powerstrip Conteg.			
SOW Annex-A	[SRS-4-221]	The Firewall components SHALL support 10GbE.			
SOW Annex-A	[SRS-4-222]	The Firewall components SHALL handle at least 90Gb throughput per 24 hour period.			
SOW Annex-A	[SRS-4-223]	The Firewall components SHALL be able to sustain, on average, at least 6Gb/s throughput.			
SOW Annex-A	[SRS-4-224]	The IEG-C_DEX SHALL preserve the Differentiated Services field (DS Field) [IETF RFC 2474, 1998] in the IPv4 and IPv6 Headers.			
SOW Annex-A	[SRS-4-225]	Unless otherwise identified during the Site Survey [SOW-673], the IEG-C and all of its components SHALL be certified to TEMPEST Level C, as defined in [SDIP-27/2].			
SOW Annex-A	[SRS-4-226]	It ~~SHALL~~ SHOULD be possible to trigger the graceful shut down from the central and local management solution.			
SOW Annex-A	[SRS-4-227]	The IEG-C shall include secure remote management capabilities providing the ability to integrate the monitoring all IEG-C components into a local NATO monitoring solution.			
SOW Annex-A	[SRS-4-228]	The IEG-C shall include secure remote management capabilities providing the ability to manage all IEG-C components locally in case of loss of connectivity with the central management system.			
SOW Annex-A	[SRS-4-229]	The IEG-C Web Proxy component SHALL support the use Simple Certificate Enrolment Protocol (SCEP) [IETF RFC 8894, 2020] to sign the impersonation certificates that are used to support the interception Transport Layer Security (TLS) version 1.2 protected web (HTTPS) traffic.			
SOW Annex-A	[SRS-4-23]	The Web Guard SHALL be connected to both the High Domain Firewall (via the High Domain Network Switch) and the Low Domain Firewall (via the Low Domain Network Switch) via separate physical interfaces.			
SOW Annex-A	[SRS-4-230]	The IEG-C Web Proxy component SHOULD support the use of Enrolment over Secure Transport (EST) [IETF RFC 7030, 2013] to sign the impersonation certificates that are used to support the interception Transport Layer Security (TLS) version 1.2 protected web (HTTPS) traffic.			
SOW Annex-A	[SRS-4-231]	The IEG-C Web Proxy component SHALL ensure HTTP request or response does not contain any of the configured words/phrases.			
SOW Annex-A	[SRS-4-232]	The IEG-C Web Proxy component SHALL inspect each of the HTTP request or response, including any attachments, for occurrences of any of the configured words/phrases.			
SOW Annex-A	[SRS-4-233]	The IEG-C Web Proxy component SHALL perform case insensitive and normalised whitespace (stripping leading and trailing white space and replacing sequences of white space characters with a single space) matching when searching for each of the configured words/phrases in the http request or response and any attachments.			
SOW Annex-A	[SRS-4-24]	The IEG-C shall include secure remote management capabilities providing the ability to monitor and control all IEG-C components remotely from central NATO management premises.			
SOW Annex-A	[SRS-4-25]	To support the (remote) management of the IEG-C, a Management Domain Network Switch SHALL be provided.			
SOW Annex-A	[SRS-4-28]	The Management Domain Network Switch SHALL be connected to the High Domain Firewall.			
SOW Annex-A	[SRS-4-29]	All IEG-C components SHALL have a connection to the Management Domain Switch.			
SOW Annex-A	[SRS-4-3]	The IEG-C architecture and all of its components SHALL be compliant with "INFOSEC Technical and Implementation Directive for the Interconnection of Communications and Information Systems (CIS)" [NAC, AC/322-D/0030-REV5.			
SOW Annex-A	[SRS-4-30]	The IEG-C wired infrastructure for connecting IEG-C components (that are required to be connected together to support the information exchange requirements for the CIS interconnection) SHALL be based on Ethernet running over fibre optic and copper cables.			
SOW Annex-A	[SRS-4-31]	The IEG-C SHALL be conformant with the service interface profiles (SIPs) and NATO Interoperability Standards and Profiles (NISPs) listed in APPENDIX B.			
SOW Annex-A	[SRS-4-32]	reserved			
SOW Annex-A	[SRS-4-33]	The IEG-C SHALL interface and function correctly with the NATO Computer Incident Response Capability (NCIRC).			
SOW Annex-A	[SRS-4-34]	The IEG-C SHALL interface and function correctly with the NATO Enterprise Service Management and Control (SMC) capability.			
SOW Annex-A	[SRS-4-35]	The IEG-C SHALL interface and function correctly with the NATO Public Key Infrastructure (NPKI) capability.			
SOW Annex-A	[SRS-4-36]	The IEG-C SHALL interface and function correctly with the NATO Enterprise Directory Services (NEDS) capability.			
SOW Annex-A	[SRS-4-37]	The IEG-C SHALL interface and function correctly with the ON AIS and MS AIS Active Directory Domain Services (ADDS) capability.			
SOW Annex-A	[SRS-4-38]	The IEG-C SHALL interface and function correctly with the Operational Network (ON) Automated Information System (AIS) and Mission Secret (MS) AIS mail exchange capability.			
SOW Annex-A	[SRS-4-39]	The IEG-C SHALL interface and function correctly with the ON AIS and MS AIS Domain Name Services (DNS) capability.			
SOW Annex-A	[SRS-4-4]	The IEG-C and all of its components SHALL be configured in accordance with the "Technical and Implementation Directive for CIS Security" [NAC AC/322-D/0048-REV3, 2019].			
SOW Annex-A	[SRS-4-40]	The IEG-C SHALL use fully qualified domain names (FQDN, [IETF RFC 1983, 1996]) for identifying all hosts, unless specifically requested not to.			
SOW Annex-A	[SRS-4-41]	The IEG-C SHALL interface and function correctly with the ON AIS and MS AIS web client and server capability providing SOAP-based and REST-based web services.			
SOW Annex-A	[SRS-4-42]	The IEG-C SHALL interface and function correctly with the ON AIS and MS AIS web client and server capability providing web browsing.			
SOW Annex-A	[SRS-4-43]	~~The IEG-C SHALL interface and function correctly with the ON AIS and MS AIS Collaboration Services capability providing audio, voice and video services.~~			
SOW Annex-A	[SRS-4-44]	The IEG-C SHALL interface and function correctly with the ON AIS Information Exchange Gateway Functional Services (IEG-FS) Extensible Messaging and Presence Protocol (XMPP) capability for exchanging text-based collaboration services messages.			
SOW Annex-A	[SRS-4-45]	The IEG-C SHALL interface and function correctly with the ON AIS Information Exchange Gateway Functional Services (IEG-FS) Tactical Data Link (TDL) capability for exchanging TDL-formatted messages.			
SOW Annex-A	[SRS-4-46]	The IEG-C SHALL interface and function correctly with the ON AIS Information Exchange Gateway Functional Services (IEG-FS) Friendly Force Tracking (FFT) capability for exchanging FFT-formatted messages.			
SOW Annex-A	[SRS-4-48]	The IEG-C SHALL interface and function correctly with the authoritative ON AIS Network Time Protocol (NTP) source.			
SOW Annex-A	[SRS-4-49]	The IEG-C Firewall components (High Domain Firewall and Low Domain Firewall) SHALL be the: • Palo Alto Networks PA-3260 with redundant AC power supplies			
SOW Annex-A	[SRS-4-5]	~~All~~ IEG-C components ~~SHALL~~ SHOULD gracefully shut down on notification from the Uninterruptible Power Supply (UPS).			
SOW Annex-A	[SRS-4-51]	The IEG-C High Domain Firewall component Network Time Protocol (NTP) server SHALL be synchronized to a designated NTP server in the ON AIS domain.			
SOW Annex-A	[SRS-4-52]	The IEG-C High Domain Firewall component SHALL be configured as the Authoritative Network Time Protocol (NTP) source for all IEG-C components (including the Low Domain Firewall) that require to be time synchronised.			
SOW Annex-A	[SRS-4-53]	The IEG-C High Domain Firewall and IEG-C Low Domain Firewall components SHALL enable the capability to support only those Data Exchange Services as specified in Table 4 (for that component).			
SOW Annex-A	[SRS-4-54]	The IEG-C High Domain Firewall and Low Domain Firewall components SHALL be configurable to support the enforcement of the following IEG-C IFPs (see Section 3.4.4): • IEG-C_IFP_CA_HL - Communications Access Services High to Low IFP; • IEG-C_IFP_CA_LH - Communications Access Services Low to High IFP; and, • IEG-C_IFP_CS_MGMT - Core Services Management Services IFP			
SOW Annex-A	[SRS-4-55]	The IEG-C High Domain Firewall and Low Domain Firewall components SHALL enable the capability to configure the IEG-C_IFP_CA_HL and IEG-C_IFP_CA_LH IFPs to allow only authorized systems/hosts to exchange data between the high domain and the low domain.			
SOW Annex-A	[SRS-4-56]	The IEG-C High Domain Firewall and Low Domain Firewall components SHALL enable the capability to configure the IEG-C_IFP_CA_HL and IEG-C_IFP_CA_LH IFPs in order to allow only those protocols and ports required to support the information exchange requirements for the high domain - low domain interconnection.			
SOW Annex-A	[SRS-4-57]	The IEG-C High Domain Firewall and Low Domain Firewall components SHALL enable the capability to configure the IEG-C_IFP_SOA_HL and the IEG-C_IFP_SOA_LH IFPs in order to route authorised HTTP(S) application-level traffic to the appropriate IEG-C guard or proxy component (through the High Side Switch or appropriate Low Side Switch depending upon the source and destination of the HTTP(S) application-level traffic) in the DMZ.			
SOW Annex-A	[SRS-4-58]	The IEG-C High Domain Firewall and Low Domain Firewall components SHALL enable the capability to configure the IEG-C_IFP_BS_HL and the IEG-C_IFP_BS_LH IFPs in order to route authorised SMTP application-level traffic to the IEG-C Mail Guard component (through the High Side Switch or appropriate Low Side Switch depending upon the source and destination of the SMTP application-level traffic) in the DMZ.			
SOW Annex-A	[SRS-4-59]	The IEG-C High Domain Firewall and Low Domain Firewall components SHALL enable the capability to configure the IEG-C_IFP_IS_HL IFP in order to route authorised RDP application-level traffic to the IEG-C RDP Proxy component (through the High Side Switch depending upon the source and destination of the RDP application-level traffic) in the DMZ.			
SOW Annex-A	[SRS-4-6]	The IEG-C SHALL provide supporting components required for the composition of an IEG-C (see Section 4.7.2).			
SOW Annex-A	[SRS-4-60]	The IEG-C High Domain Firewall and Low Domain Firewall components SHALL enable the capability to configure the IEG-C_IFP_CS_MGMT IFP in order to route authorised management traffic to the appropriate IEG-C component (through the Management Switch) in the DMZ.			
SOW Annex-A	[SRS-4-61]	The IEG-C High Domain Firewall and Low Domain Firewall components SHALL enforce the IEG-C IFPs configured (depending upon the information exchange requirements and protection policy enforced for the CIS interconnection) for the IEG-C.			
SOW Annex-A	[SRS-4-62]	The IEG-C High Domain Firewall and Low Domain Firewall components SHALL be enabled and configured with the capability for being managed as specified in Section 9.			
SOW Annex-A	[SRS-4-63]	The IEG-C High Domain Firewall component SHALL be configured to have at least three network interfaces (NICs: one for the network connection to the high domain; one for the network connection to the High Domain Switch; and, one for the network connection to the Management Domain Switch).			
SOW Annex-A	[SRS-4-64]	The IEG-C High Domain Firewall component network interfaces to the high domain SHALL be 1000BASE-SX gigabit Ethernet interfaces.			
SOW Annex-A	[SRS-4-65]	The IEG-C High Domain Firewall component network interfaces to the High Domain Switch SHALL be 1000BASE-SX gigabit Ethernet interfaces.			
SOW Annex-A	[SRS-4-66]	The IEG-C High Domain Firewall component network interface to the Management Domain Switch SHALL be a 1000-Base-SX gigabit Ethernet interface.			

SOW Annex-A	[SRS-4-67]	The IEG-C Network Switch components (High Domain, Low Domain and Management) SHALL be selected from the following list of products, equivalent or better ones: • Dell Networking N1124T Switch • Dell Networking S3048 Switch • Dell Networking S3124F Switch • Dell Networking S3148P Switch			
SOW Annex-A	[SRS-4-68]	The IEG-C Network Switch components SHALL be synchronised to the IEG-C High Domain Firewall component NTP source.			
SOW Annex-A	[SRS-4-69]	The IEG-C Network Switch components SHALL enable the Data Exchange Services as specified in Table 4 (for that component).			
SOW Annex-A	[SRS-4-7]	IEG-C_DEX SHALL offer User Datagram Protocol (UDP) [IETF RFC 768, 1980] and Internet Protocol (IP), IPv4 and IPv6, [IETF RFC 791, 1981], [IETF RFC 8200, 2017] over Ethernet interfaces 'Communications Access Services HL' and 'Communications Access Services LH' on top of IEG-C_IF_NET_HIGH and IEG-C_IF_NET_LOW, respectively.			
SOW Annex-A	[SRS-4-70]	The IEG-C High Domain Network Switch and Low Domain Network Switch components SHALL be enabled and configured with the capability for being managed as specified in Section 9.			
SOW Annex-A	[SRS-4-71]	The IEG-C High Domain Switch component SHALL be configured to have at least five network interfaces (NICs: one for the network connection to the High Domain Firewall; one for the network connection to the Mail Guard; one for the network connection to the Web Guard; one for the network connection to the server component; and, one for the network connection to the Management Domain Switch).			
SOW Annex-A	[SRS-4-72]	The IEG-C High Domain Network Switch component network interface to the high domain firewall SHALL be 1000BASE-SX gigabit Ethernet interface.			
SOW Annex-A	[SRS-4-73]	The IEG-C High Domain Network Switch component network interfaces to the Mail Guard, Web Guard, server component and Management Domain Switch SHALL be 1000BASE-SX gigabit Ethernet interfaces.			
SOW Annex-A	[SRS-4-74]	The IEG-C Low Domain Switch components SHALL be configured to have at least five network interfaces (NICs: one for the network connection to the Low Domain firewall; one for the network connection to the Mail Guard; one for the network connection to the Web Guard; one for the network connection to the server component; and, one for the network connection to the Management Domain Switch).			
SOW Annex-A	[SRS-4-75]	The IEG-C Low Domain Network Switch component network interface to the Low Domain Firewall SHALL be 1000BASE-SX gigabit Ethernet interface.			
SOW Annex-A	[SRS-4-76]	The IEG-C Low Doman Network Switch component network interfaces to the Mail Guard, Web Guard, server component and Management Domain Switch SHALL be 1000BASE-SX gigabit Ethernet interfaces.			
SOW Annex-A	[SRS-4-77]	The IEG-C Management Domain Switch component SHALL be configured to have at least seven network interfaces (NICs: one for the network connection to the High Domain Firewall; one for the network connection to the Mail Guard; one for the network connection to the Web Guard; one for the network connection to the server component; one for the network connection to the High Domain Network Switch, one for the network connections to the Low Domain Network Switch and one for the network connection to the Low Domain Firewall).			
SOW Annex-A	[SRS-4-78]	The IEG-C Management Domain Network Switch component network interface to the Firewall SHALL be a 1GbE interface.			
SOW Annex-A	[SRS-4-79]	The IEG-C Management Domain Network Switch component network interfaces to the Mail Guard, Web Guard, server component, High Domain Switch and Low Domain Switches SHALL be 1GbE interfaces.			
SOW Annex-A	[SRS-4-8]	IEG-C_DEX SHALL offer HyperText Transport Protocol (HTTP), v1.1 and v2, [IETF RFC 7230, 2014], [IETF RFC 7540, 2014] interface 'SOA Platform Services HL' on top of 'Communications Access Services HL' and HyperText Transport Protocol (HTTP), v1.1 and v2. [IETF RFC 7230, 2014],[IETF RFC 7540, 2014] interface 'SOA Platform Services LH' on top of 'Communications Access Services LH'.			
SOW Annex-A	[SRS-4-81]	The IEG-C Web Proxy component SHALL be synchronised to the IEG-C High Domain Firewall component NTP source.			
SOW Annex-A	[SRS-4-82]	The IEG-C Web Proxy component SHALL enable the capability to support only those Data Exchange Services as specified in Table 4 (for that component).			
SOW Annex-A	[SRS-4-83]	The IEG-C Web Proxy component SHALL enable the capability to perform cryptographic operations and key management to support interception of Transport Layer Security (TLS) version 1.2 protected web (HTTPS) traffic.			
SOW Annex-A	[SRS-4-84]	The IEG-C Web Proxy component SHALL be configured to conform to the INFOSEC CIS Security Technical and Implementation Guidance in Support of Public Key Infrastructure - Cryptographic Aspects [NAC AC/322-D(2007)0002-REV1, 2015].			
SOW Annex-A	[SRS-4-85]	The IEG-C Web Proxy component SHALL be configured to conform to the INFOSEC Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanisms [NAC AC/322-D/0047-REV2 (INV), 2009].			
SOW Annex-A	[SRS-4-86]	The IEG-C Web Proxy component provided cryptographic mechanism SHALL be configured based on Technical Implementation Guidance on Cryptographic Mechanisms in Support of Cryptographic Services [NAC AC/322-D(2012)0022, 2013].			
SOW Annex-A	[SRS-4-87]	The IEG-C Web Proxy component SHALL use a malware/virus scanner that is included in the NATO Information Assurance Product Catalogue (NIAPC) to check web content for malicious content.			
SOW Annex-A	[SRS-4-89]	The IEG-C Web Proxy components SHALL enable the capability to be configured as a reverse web proxy from the high domain to the low domain.			
SOW Annex-A	[SRS-4-9]	The 'SOA Platform Services HL' and 'SOA Platform Services LH' interfaces SHALL support Transport Layer Security (TLS, [IETF RFC 8446, 2018]).			
SOW Annex-A	[SRS-4-90]	The IEG-C Web Proxy component SHALL be configurable to support the enforcement of the following IEG-C SOA Platform IFPs (see Section 3.4.4): • IEG-C_IFP_SOA_HL - SOA Platform Services High to Low IFP; and, • IEG-C_IFP_SOA_LH - SOA Platform Services Low to High IFP.			
SOW Annex-A	[SRS-4-91]	The IEG-C Web Proxy component SHALL be configurable to support the enforcement of the following IEG-C SOA Platform CIP (see Section 3.4.5): • IEG-C_CIP_SOA_LH - SOA Platform Services Low to High CIP.			
SOW Annex-A	[SRS-4-92]	The IEG-C Web Proxy component SHALL enable the capability to configure the IEG-C_IFP_SOA_HL IFP in order to guard HTTP application-level web browsing requests from the high domain to the low domain.			
SOW Annex-A	[SRS-4-93]	The IEG-C Web Proxy component SHALL enable the capability to configure the IEG-C_IFP_SOA_LH IFP in order to guard HTTP application-level web browsing responses from the low domain to the high domain.			
SOW Annex-A	[SRS-4-94]	The IEG-C Web Proxy component SHALL enable the capability to configure the IEG-C_IFP_SOA_HL and IEG-C_IFP_SOA_LH IFPs to verify that the HTTP request (from the high domain to the low domain) and HTTP response (from the low domain to the high domain) can be released by checking high domain web client access control rules against white or black lists (assuring only authorised high domain clients (or users) have access to the low domain web content).			
SOW Annex-A	[SRS-4-95]	The IEG-C Web Proxy component SHALL enable the capability to configure the IEG-C_IFP_SOA_HL and IEG-C_IFP_SOA_LH IFPs to verify that the HTTP request (from the high domain to the low domain) and HTTP response (from the low domain to the high domain) can be released by checking low domain web server access control rules against white or black lists (assuring only authorised low domain web servers are published and made accessible for high domain clients).			
SOW Annex-A	[SRS-4-96]	The IEG-C Web Proxy component SHALL enable the capability to configure the IEG-C_IFP_SOA_LH IFP to enforce the IEG-C_CIP_SOA_LH CIP.			
SOW Annex-A	[SRS-4-97]	The IEG-C Web Proxy component SHALL enable the capability to configure the IEG-C_CIP_SOA_LH CIP to verify that all HTTP responses from the low domain to the high domain (to HTTP requests from the high domain to the low domain) do not contain any disallowed attachment types by checking against a white list or black list of attachment types.			
SOW Annex-A	[SRS-4-98]	The IEG-C Web Proxy component SHALL enable the capability to configure the IEG-C_CIP_SOA_LH CIP to verify that all HTTP responses from the low domain to the high domain (to HTTP requests from the high domain to the low domain) contain no malicious content.			
SOW Annex-A	[SRS-4-99]	The IEG-C Web Proxy component SHALL enforce the IEG-C SOA Platform IFPs and SOA Platform CIP configured (depending upon the information exchange requirements and protection policy enforced for the CIS interconnection) for the IEG-C.			
SOW Annex-A	[SRS-5-1]	The IEG-C SHALL have all functionality ready to use for an authorised user after invoking the system function within 5 minutes.			
SOW Annex-A	[SRS-5-10]	The IEG-C SHALL be able to support additional system resources (introduction of additional storage capacity or server processing power) without having to modify the system architecture, replace existing components, interrupt or degrade current functional and performance requirements.			
SOW Annex-A	[SRS-5-100]	The IEG-C SHALL be composed of discrete components such that a change to one component has minimal impact on other components.			
SOW Annex-A	[SRS-5-101]	The IEG-C SHALL be able to report its status (healthy, warnings, errors) and 'capacity' related aspects for the [IT] resources used (disk, memory, CPU, network) and the application aspects addressed (load, transactions, users) to the NATO EMS environment (in addition to any project specific requirements).			
SOW Annex-A	[SRS-5-102]	The IEG-C SHALL ensure that the application provides management of Personal Information (e.g., User profile and expertise information) held within the IEG-C.			
SOW Annex-A	[SRS-5-103]	The IEG-C SHALL support remote configuration of all IEG-C components and updates using Microsoft System Center Configuration Manager (SCOM) if available on the platform.			
SOW Annex-A	[SRS-5-104]	IEG-C software assets (including different versions) SHALL have a unique SWID tag assigned.			
SOW Annex-A	[SRS-5-105]	The IEG-C SHALL support collection and reporting of asset inventory metrics for all IEG-C components using Microsoft System Centre Configuration Manager, unless an IEG-C component does not support SCOM, including: • Memory • Operating System • Peripherals • Services • Login tracking • Software existence and usage • Licensing			
SOW Annex-A	[SRS-5-106]	The IEG-C SHALL be effective and efficient in the adaptation for different or evolving hardware, software or other operational or usage environments.			

SOW Annex-A	[SRS-5-107]	The IEG-C architecture SHALL be designed to permit upgrading for use of new communication, processing and storage technologies during its operational lifetime.			
SOW Annex-A	[SRS-5-108]	The IEG-C SHALL be equipped with an Installation Guide.			
SOW Annex-A	[SRS-5-109]	The IEG-C Installation Guide SHALL explain all actions to take in order to install and configure the IEG-C, including COTS components. Every action SHALL be followed by a description (text and/or screenshots) of the feedback which will be displayed.			
SOW Annex-A	[SRS-5-11]	The IEG-C SHALL use the existing interoperability profiles and provide any new profiles into the NATO Interoperability Standards and Profiles [ADatP-34] (NISP) volumes after all implementation is completed.			
SOW Annex-A	[SRS-5-110]	The IEG-C Installation Guide SHALL describe:			
SOW Annex-A	[SRS-5-111]	The IEG-C Installation Guide SHALL describe how to configure the system backbone to be able to run the IEG-C.			
SOW Annex-A	[SRS-5-112]	The IEG-C Installation Guide SHALL contain a description of all configuration files. The following points SHALL be described: • The location of the configuration file • The content of the configuration file • The available settings of the items in the configuration file and their meaning • How to change the configuration file			
SOW Annex-A	[SRS-5-113]	Two copies of the SWID tag file SHALL be installed on each system that the IEG-C software is installed on. The first copy of the tag file SHALL be accessible in the top level directory of the installed software package itself and the second copy of the tag file SHALL be installed in a platform dependent file system location as: <file system location>\regid.1997-08.int.nato\<tagfilename>."			
SOW Annex-A	[SRS-5-114]	The IEG-C SHALL provide a capability to completely uninstall IEG-C application(s)/component(s). The IEG-C uninstallation capability SHALL remove all program files and folders, registry entries, program and group folders, as appropriate, retaining all shared and system files.			
SOW Annex-A	[SRS-5-115]	The IEG-C uninstallation capability SHALL not adversely impact other installed applications.			
SOW Annex-A	[SRS-5-116]	The IEG-C SHALL store IEG-C temporary files only in the IEG-C's temporary folders in configurable locations.			
SOW Annex-A	[SRS-5-117]	An IEG-C System Administrator SHALL be able to successfully deploy (i.e., install and configure) a component in the IEG-C within a time frame of one (1) working day after receiving a maximum of five (5) days of training per component.			
SOW Annex-A	[SRS-5-118]	All software and documentation to be provided by the Contractor under this project SHALL be in English (US) version.			
SOW Annex-A	[SRS-5-119]	The IEG-C SHALL automatically detect the availability and re-establishment of network connectivity and SHALL initiate subsequent tasks as though network connectivity had not been lost.			
SOW Annex-A	[SRS-5-12]	The IEG-C software code and components SHALL comply with the latest version of the NATO Interoperability Standards and Profiles (NISP). Any deviation is to be justified and reviewed by the Technical Project Board.			
SOW Annex-A	[SRS-5-121]	The IEG-C SHALL support the use of IPv6 without impaired functionality and performance within a network environment.			
SOW Annex-A	[SRS-5-122]	The IEG-C SHALL be compliant to the requirements specified in this SRS in a virtualized server environment (virtual servers).			
SOW Annex-A	[SRS-5-123]	The IEG-C equipment SHALL NOT be damaged nor suffer loss of data, when any of the ambient temperature and humidity conditions contravene operating limits while power is available.			
SOW Annex-A	[SRS-5-124]	The IEG-C support staff SHALL be able to manually resume normal operation of the IEG-C equipment within five (5) minutes from when ambient temperature and humidity conditions return to within operating limits.			
SOW Annex-A	[SRS-5-125]	The WG SHALL support the concurrent processing of low-to-high and high-to-low traffic and meet the performance objectives for both traffic flows.			
SOW Annex-A	[SRS-5-126]	The WG SHALL support the concurrent execution of low-to-high and high-to-low policy enforcement and meet the performance objectives for each.			
SOW Annex-A	[SRS-5-127]	The WG SHALL support the concurrent execution of all functionality offered by the building blocks Data Exchange Services, Protection Policy Enforcement Services, Protection Services and Element Management Services.			
SOW Annex-A	[SRS-5-128]	On interface WG_IF_NET_HIGH (see 6.4.1.2) the WG SHALL be capable of handling at least 50 concurrent receive connections and 50 concurrent send side connections.			
SOW Annex-A	[SRS-5-129]	On interface WG_IF_NET_LOW (see 6.4.1.3) the WG SHALL be capable of handling at least 50 concurrent receive connections and 50 concurrent send side connections.			
SOW Annex-A	[SRS-5-13]	The IEG-C SHALL be compliant with NATO document AC/35-D/2002 "Directive on Security of Information".			
SOW Annex-A	[SRS-5-131]	The WG SHALL allow an IEG-C System Administrator to perform system management functions regardless of the load on the WG.			
SOW Annex-A	[SRS-5-132]	The WG SHALL support the information exchange of HTTP messages with body size up to ten (10) GB.			
SOW Annex-A	[SRS-5-133]	The WG SHALL support parallel processing of HTTP messages, i.e. it SHALL be possible for the WG to subject multiple different HTTP messages to policy enforcement at the same time.			
SOW Annex-A	[SRS-5-134]	The WG SHALL support[3] the following normal loads per message size category: • Very small HTTP messages: a SCNL of 35000 HTTP messages per minute with average message size 15 KB. • Small HTTP messages: a SCNL of 180 HTTP messages per minute with average message size 5 MB. • Medium HTTP messages: a SCNL of 30 HTTP messages per minute with average message size 30 MB. • Large HTTP messages: a SCNL of 10 HTTP messages per minute with average message size 70 MB. • Very large HTTP messages: a SCNL of 2 HTTP messages per minute with average message size 300 MB.			
SOW Annex-A	[SRS-5-135]	The WG SHALL meet the requirements in [SRS-5-133] under a total normal load *TNL* with the following constraints on the *TNL* characteristics: • TNL average message size < 7 MB; • TNL maximum message size <= 10 GB; • TNL message size distribution: 80% of TNL < 150 KB; 95% of TNL < 30 MB; 98% of TNL < 300 MB.			
SOW Annex-A	[SRS-5-136]	Per size category the average *HTTP message processing time T_WG_Proc-Average* SHALL meet the following constraints under the size category normal loads from [SRS-5-133]: • Very small HTTP messages: T_WG_Proc-Average < 200 milliseconds; • Small HTTP messages: T_WG_Proc-Average < 3000 milliseconds; • Medium HTTP messages: T_WG_Proc-Average < 15000 milliseconds; • Large HTTP messages: T_WG_Proc-Average < 60000 milliseconds; • Very large HTTP messages: T_WG_Proc-Average < 240000 milliseconds.			
SOW Annex-A	[SRS-5-137]	The WG SHALL meet the requirements on *HTTP message processing time* in [SRS-5-135] under a total normal load *TNL* with the following constraints on the *TNL* characteristics: • TNL average message size < 7 MB; • TNL maximum message size <= 10 GB; • TNL message size distribution: 80% of TNL < 150 KB; 95% of TNL < 30 MB; 98% of TNL < 300 MB.			
SOW Annex-A	[SRS-5-138]	If an HTTP message *H* is processed by the WG that is too large for the category 'Very large HTTP messages', the WG SHALL: • continue to operate; • be responsive to commands issued by a System Administrator; • meet the requirements in [SRS-5-133] under the total normal load TNL; • and MAY terminate the processing of H in order to do so.			
SOW Annex-A	[SRS-5-139]	If, while under the total normal load *TNL* , a peak load occurs for one of the size categories, the average *WG throughput* for that size category SHALL meet the following constraints for the peak load stated, while not rejecting HTTP traffic: • Very small HTTP messages: for a peak load of 2 times the number of messages in the SCNL with a duration of 300 seconds, the average throughput SHALL decrease at most 10% when compared to the SCNL. • Small HTTP messages: for a peak load of 2 times the number of messages in the SCNL with a duration of 300 seconds, the average throughput SHALL decrease at most 10% when compared to the SCNL. • Medium HTTP messages: for a peak load of 2 times the number of messages in the SCNL with a duration of 300 seconds, the average throughput SHALL decrease at most 10% when compared to the SCNL. • Large HTTP messages: for a peak load of 2 times the number of messages in the SCNL with a duration of 300 seconds, the average throughput SHALL decrease at most 10% when compared to the SCNL. • Very large HTTP messages: for a peak load of 2 times the number of messages in the SCNL with a duration of 300 seconds, the average throughput SHALL decrease at most 10% when compared to the SCNL.			
SOW Annex-A	[SRS-5-14]	The IEG-C SHALL comply with NATO document "Primary Directive on CIS Security" [AC/35-D/2004-REV3].			
SOW Annex-A	[SRS-5-140]	If, while under the total normal load *TNL* , a peak load occurs for one of the size categories, the average *HTTP message forwarding time T_WG_Forward-Average* for that size category SHALL satisfy the following conditions for the peak load stated, while not rejecting HTTP traffic: • Very small HTTP messages: for a peak load of 2 times the number of messages in the SCNL with a duration of 300 seconds, T_WG_Forward-Average SHALL increase at most 10% when compared to the SCNL. • Small HTTP messages: for a peak load of 2 times the number of messages in the SCNL with a duration of 300 seconds, T_WG_Forward-Average SHALL increase at most 20% when compared to the SCNL. • Medium HTTP messages: for a peak load of 2 times the number of messages in the SCNL with a duration of 300 seconds, T_WG_Forward-Average SHALL increase at most 30% when compared to the SCNL.' • Large HTTP messages: for a peak load of 2 times the number of messages in the SCNL with a duration of 300 seconds, T_WG_Forward-Average SHALL increase at most 40% when compared to the SCNL. • Very large HTTP messages: for a peak load of 2 times the number of messages in the SCNL with a duration of 300 seconds, T_WG_Forward-Average SHALL increase at most 50% when compared to the SCNL.			

SOW Annex-A	[SRS-5-141]	If, while under the total normal load *TNL* , a peak load occurs for one of the size categories, the average *HTTP message processing time T_WG_Proc-Average* for that size category SHALL satisfy the following conditions for the peak load stated, while not rejecting HTTP traffic: • Very small HTTP messages: for a peak load of 2 times the number of messages in the SCNL with a duration of 300 seconds, T_WG_Proc-Average SHALL increase at most 5% compared to normal load. • Small HTTP messages: for a peak load of 2 times the number of messages in the SCNL with a duration of 300 seconds, T_WG_Proc-Average SHALL increase at most 10% compared to normal load. • Medium HTTP messages: for a peak load of 2 times the number of messages in the SCNL with a duration of 300 seconds, T_WG_Proc-Average SHALL increase at most 20% compared to normal load. • Large HTTP messages: for a peak load of 2 times the number of messages in the SCNL with a duration of 300 seconds, T_WG_Proc-Average SHALL increase at most 30% compared to normal load. • Very large HTTP messages: for a peak load of 2 times the number of messages in the SCNL with a duration of 300 seconds, T_WG_Proc-Average SHALL increase at most 40% compared to normal load.			
SOW Annex-A	[SRS-5-142]	During peak loads that are larger in size or longer in duration than those specified in [SRS-5-138] , [SRS-5-139] and [SRS-5-140] , the WG SHALL continue to operate and be responsive to commands issued by a System Administrator, and MAY reject HTTP traffic in order to do so.			
SOW Annex-A	[SRS-5-143]	If peak loads for multiple size categories take place simultaneously, the WG SHALL continue to operate and be responsive to commands issued by a System Administrator, and MAY reject HTTP traffic in order to do so.			
SOW Annex-A	[SRS-5-144]	It SHALL be possible to configure an upper size limit, L, such that the WG SHALL reject messages that exceed L.			
SOW Annex-A	[SRS-5-145]	The impact of logging by the WG on its performance SHALL remain within the following limits, for the following log severity levels [RFC 5424]: • For severity levels 'Emergency' (0), 'Alert' (1), 'Critical' (2), 'Error' (3), 'Warning' (4): no impact on performance; • For severity levels 'Notice' (5) and 'Informational' (6): a decrease in throughput of at most 40%. • For severity level 'Debug' (7): a decrease in throughput of at most 80%.			
SOW Annex-A	[SRS-5-146]	The WG SHALL be scalable such that when an increase in traffic occurs, capacity can be increased in order to keep meeting the requirements on Time Behaviour in 5.3.1.2.			
SOW Annex-A	[SRS-5-147]	The WG ~~architecture~~ SHALL support horizontal scalability and allow for multiple instances of the WG to be deployed on multiple machines, supporting the information exchange requirements in concert.			
SOW Annex-A	[SRS-5-148]	The WG ~~SHALL~~ SHOULD be vertically scalable, i.e. the WG ~~SHALL~~ SHOULD be able to adapt its performance characteristics by having additional system resources added such as processing power, memory, disk capacity, or network capacity.			
SOW Annex-A	[SRS-5-149]	In order to keep meeting the requirements on Time Behaviour in 5.3.1.2 it SHALL be possible to apply horizontal scalability without disrupting the services offered by any active WG.			
SOW Annex-A	[SRS-5-15]	The IEG-C SHALL be compliant with the NATO document "INFOSEC Technical and Implementation Directive on the Requirement for, and the Selection, Approval and Implementation of, Security Tools (ST)" [AC/322-D(2004)0030].			
SOW Annex-A	[SRS-5-150]	The horizontal scaling of the WG SHALL NOT introduce any additional WG management overhead.			
SOW Annex-A	[SRS-5-151]	The WG SHALL be dimensioned and configured to be able to scale in performance and support the following per a year for three years without degradation of performance as specified in section 5.3.1.2: • a 200% increase in the SCNL (normal load for each HTTP message size category); • a 50% increase in message size.			
SOW Annex-A	[SRS-5-152]	~~The WG SHALL have a high degree of learnability, making it very easy to use for System Administrators even the first time.~~			
SOW Annex-A	[SRS-5-153]	The WG SHALL score above 80% in user success rate without external support, for System Administrators that have received standard training.			
SOW Annex-A	[SRS-5-156]	The WG SHALL notify a System Administrator by e-mail when the audit log reaches 75% of its maximum permitted size.			
SOW Annex-A	[SRS-5-157]	The WG SHALL provide a configuration option to set the maximum permitted size of the audit log.			
SOW Annex-A	[SRS-5-158]	The WG SHALL contain residual information protection mechanisms to ensure that purged information is no longer accessible.			
SOW Annex-A	[SRS-5-159]	The WG SHALL ensure that newly created objects do not contain information that should not be accessible (i.e. information that has been logically deleted).			
SOW Annex-A	[SRS-5-161]	WG log messages SHALL contain initiating module information, Date/Time (Z), system instance, (log) message, category/severity, user (invoker of function), and context information (like mission/session, service/function, parameters, and trace-log).			
SOW Annex-A	[SRS-5-162]	A WG System Administrator SHALL be able to successfully deploy (i.e., install and configure to a predefined configuration) the WG within a time frame of one (1) working days after receiving a maximum of five (5) days of training.			
SOW Annex-A	[SRS-5-166]	Any IEG-C component SHALL not exceed 2U height. If it is determined (by analysis and/or empirically) that this is not feasible, any deviation request shall be submitted to Purchaser approval.			
SOW Annex-A	[SRS-5-17]	The IEG-C SHALL be compliant with NATO document "Security within the North Atlantic Treaty Organisation" [NAC C-M(2002)49-COR12].			
SOW Annex-A	[SRS-5-18]	The IEG-C SHALL guarantee all incoming and outgoing formatted messages are valid according to the specified formats.			
SOW Annex-A	[SRS-5-19]	The IEG-C primary security services (access control, confidentiality, integrity, authentication, and non-repudiation) SHALL be supported by X.509			
SOW Annex-A	[SRS-5-2]	The IEG-C SHALL execute the log-in function within 30 seconds.			
SOW Annex-A	[SRS-5-20]	The IEG-C X.509 support to primary security services SHALL be compliant with NPKI.			
SOW Annex-A	[SRS-5-208]	The MG SHALL support the concurrent processing of low-to-high and high-to-low traffic and meet the performance objectives for both traffic flows.			
SOW Annex-A	[SRS-5-209]	The MG SHALL support the concurrent execution of low-to-high and high-to-low policy enforcement and meet the performance objectives for each.			
SOW Annex-A	[SRS-5-21]	The IEG-C SHALL use country codes according to "Letter Codes for Geographical Entities" [STANAG 1059].			
SOW Annex-A	[SRS-5-210]	The MG SHALL support the concurrent execution of all functionality offered by the building blocks Data Exchange Services, Protection Policy Enforcement Services, Protection Services and Element Management Services.			
SOW Annex-A	[SRS-5-211]	On interface MG_IF_NET_HIGH (see section 7.1.2) the MG SHALL be capable of handling at least 50 concurrent receive connections and 50 concurrent send side connections.			
SOW Annex-A	[SRS-5-212]	On interface MG_IF_NET_LOW (see section 7.1.2) the MG SHALL be capable of handling at least 50 concurrent receive connections and 50 concurrent send side connections.			
SOW Annex-A	[SRS-5-213]	The MG SHALL queue SMTP messages in the event that policy enforcement functionality is unavailable.			
SOW Annex-A	[SRS-5-214]	The MG SHALL allow an IEG-C System Administrator to perform system management functions regardless of the load on the MG.			
SOW Annex-A	[SRS-5-215]	The MG SHALL support the information exchange of SMTP messages with body size up to ten (10) MB.			
SOW Annex-A	[SRS-5-216]	The MG SHALL support parallel processing of SMTP messages, i.e. it SHALL be possible for the MG to subject multiple different SMTP messages to policy enforcement at the same time.			
SOW Annex-A	[SRS-5-217]	The MG SHALL support[1] a total normal load, TNL, with the following normal loads per message size category: • Small SMTP messages: a SCNL of 22 SMTP messages per minute with average message size 70 KB. • Medium SMTP messages: a SCNL of 4 SMTP messages per minute with average message size 250 KB. • Large SMTP messages: a SCNL of 1 SMTP messages per minute with average message size 1 MB.			
SOW Annex-A	[SRS-5-218]	The MG SHALL support the total normal load *TNL* with the following constraints on the *TNL* characteristics: • TNL average message size < 250 KB; • TNL maximum message size <= 10 MB; • TNL message size distribution: 80% of TNL < 100 KB; 95% of TNL < 500 KB; 98% of TNL < 2.5 MB.			
SOW Annex-A	[SRS-5-219]	Per size category the average *SMTP message processing time T_MG_Proc-Average* SHALL meet the following constraints under the size category normal loads from [SRS-5-217]: • Small SMTP messages: T_MG_Proc-Average < 200 milliseconds; • Medium SMTP messages: T_MG_Proc-Average < 3000 milliseconds; • Large SMTP messages: T_MG_Proc-Average < 15000 milliseconds;			
SOW Annex-A	[SRS-5-22]	The IEG-C SHALL provide accuracy of timing for messaging time stamps (e.g., time of receipt, send, release authorisation, etc.) to one millisecond. Other system-level functions (e.g., process synchronisation) may require additional accuracy as required for correct operation.			
SOW Annex-A	[SRS-5-220]	The MG SHALL meet the requirements on *SMTP message processing time* in [SRS-5-219] under a total normal load *TNL* with the following constraints on the *TNL* characteristics: • TNL average message size < 250 KB; • TNL maximum message size <= 1 MB; • TNL message size distribution: 80% of TNL < 100 KB; 95% of TNL < 500 KB; 98% of TNL < 2.5 MB.			
SOW Annex-A	[SRS-5-221]	If an SMTP message *M* is processed by the MG that is too large for the category 'Large SMTP messages', the MG SHALL: • continue to operate; • be responsive to commands issued by a System Administrator; • meet the requirements in [SRS-5-219] under the total normal load TNL; • and MAY terminate the processing of M in order to do so.			
SOW Annex-A	[SRS-5-222]	If, while under the total normal load *TNL* , a peak load occurs for one of the size categories, the average *MG throughput* for that size category SHALL meet the following constraints for the peak load stated, while not rejecting SMTP traffic: • Small SMTP messages: for a peak load of 2 times the number of messages in the SCNL with a duration of 300 seconds, the average throughput SHALL decrease at most 10% when compared to the SCNL. • Medium SMTP messages: for a peak load of 2 times the number of messages in the SCNL with a duration of 300 seconds, the average throughput SHALL decrease at most 10% when compared to the SCNL. • Large SMTP messages: for a peak load of 2 times the number of messages in the SCNL with a duration of 300 seconds, the average throughput SHALL decrease at most 10% when compared to the SCNL.			

SOW Annex-A	[SRS-5-223]	If, while under the total normal load *TNL* , a peak load occurs for one of the size categories, the average *SMTP message forwarding time T_MG_Forward-Average* for that size category SHALL satisfy the following conditions for the peak load stated, while not rejecting SMTP traffic: • Small SMTP messages: for a peak load of 2 times the number of messages in the SCNL with a duration of 300 seconds, T_MG_Forward-Average SHALL increase at most 20% when compared to the SCNL. • Medium SMTP messages: for a peak load of 2 times the number of messages in the SCNL with a duration of 300 seconds, T_MG_Forward-Average SHALL increase at most 30% when compared to the SCNL. • Large SMTP messages: for a peak load of 2 times the number of messages in the SCNL with a duration of 300 seconds, T_MG_Forward-Average SHALL increase at most 40% when compared to the SCNL.			
SOW Annex-A	[SRS-5-224]	If, while under the total normal load *TNL* , a peak load occurs for one of the size categories, the average *SMTP message processing time T_MG_Proc-Average* for that size category SHALL satisfy the following conditions for the peak load stated, while not rejecting SMTP traffic: • Small SMTP messages: for a peak load of 2 times the number of messages in the SCNL with a duration of 300 seconds, T_MG_Proc-Average SHALL increase at most 10% compared to normal load. • Medium SMTP messages: for a peak load of 2 times the number of messages in the SCNL with a duration of 300 seconds, T_MG_Proc-Average SHALL increase at most 20% compared to normal load. • Large SMTP messages: for a peak load of 2 times the number of messages in the SCNL with a duration of 300 seconds, T_MG_Proc-Average SHALL increase at most 30% compared to normal load.			
SOW Annex-A	[SRS-5-225]	During peak loads that are larger in size or longer in duration than those specified in [SRS-5-222], [SRS-5-223] and [SRS-5-224], the MG SHALL continue to operate and be responsive to commands issued by a System Administrator, and MAY reject SMTP traffic in order to do so.			
SOW Annex-A	[SRS-5-226]	If peak loads for multiple size categories take place simultaneously, the MG SHALL continue to operate and be responsive to commands issued by a System Administrator, and MAY reject SMTP traffic in order to do so.			
SOW Annex-A	[SRS-5-227]	It SHALL be possible to configure an upper message size limit, L, such that the MG SHALL reject messages that exceed the size limit L.			
SOW Annex-A	[SRS-5-228]	The impact of logging by the MG on its performance SHALL remain within the following limits, for the following syslog severity levels [RFC 5424]: • For severity levels 'Emergency' (0), 'Alert' (1), 'Critical' (2), 'Error' (3), 'Warning' (4): no impact on performance; • For severity levels 'Notice' (5) and 'Informational' (6): a decrease in throughput of at most 40%. • For severity level 'Debug' (7): a decrease in throughput of at most 80%.			
SOW Annex-A	[SRS-5-229]	The MG SHALL be scalable such that when an increase in traffic occurs, capacity can be increased in order to keep meeting the requirements on Time Behaviour in 5.4.1.2.			
SOW Annex-A	[SRS-5-23]	The IEG-C SHALL synchronize its internal system clocks with a source on the ON using the Network Time Protocol (NTP).			
SOW Annex-A	[SRS-5-230]	The MG architecture SHALL support horizontal scalability and allow for multiple instances of the MG to be deployed on multiple machines, supporting the information exchange requirements and MG policy in concert.			
SOW Annex-A	[SRS-5-231]	The MG SHALL be vertically scalable, i.e. the MG SHALL be able to adapt its performance characteristics by having additional system resources added such as processing power, memory, disk capacity, or network capacity.			
SOW Annex-A	[SRS-5-232]	In order to keep meeting the requirements on Time Behaviour in 5.4.1.2 it SHALL be possible to apply horizontal scalability without disrupting the services offered by any active MG.			
SOW Annex-A	[SRS-5-233]	The horizontal scaling of the MG SHALL NOT introduce any additional MG management overhead.			
SOW Annex-A	[SRS-5-234]	~~The MG SHALL have a high degree of learnability, making it very easy to use for System Administrators even the first time.~~			
SOW Annex-A	[SRS-5-235]	The MG SHALL score above 80% in user success rate without external support, for System Administrators that have received standard training.			
SOW Annex-A	[SRS-5-236]	The MG SHALL continue to receive and queue messages in the event of unavailability of recipient side networking.			
SOW Annex-A	[SRS-5-237]	The MG SHALL continue to dequeue and send messages in the event of unavailability of originator side networking.			
SOW Annex-A	[SRS-5-238]	The MG SHALL notify a System Administrator by e-mail when the audit log reaches 75% of its maximum permitted size.			
SOW Annex-A	[SRS-5-239]	The MG SHALL provide a configuration option to set the maximum permitted size of the audit log.			
SOW Annex-A	[SRS-5-24]	The visual design of the IEG-C SHOULD follow the recommendations and guidelines stated in the following Documents: • NATO Visual Identity Guidelines [NATO VIG v3]			
SOW Annex-A	[SRS-5-240]	The MG SHALL contain residual information protection mechanisms to ensure that purged information is no longer accessible.			
SOW Annex-A	[SRS-5-241]	The MG SHALL ensure that newly created objects do not contain information that has been purged.			
SOW Annex-A	[SRS-5-242]	Alert messages triggered by the MG (e.g., error, warning, notification and informational messages) SHALL contain initiating module information, context sensitive help or directives on where to find answers and solutions.			
SOW Annex-A	[SRS-5-243]	MG log messages SHALL contain initiating module information, Date/Time(Z), system instance, (log) message, category/severity, user (invoker of function), context information (for example, mission/session, service/function, parameters, and trace-log).			
SOW Annex-A	[SRS-5-25]	The IEG-C icons included in the designed solution SHALL be compliant with the ISO 18152 standard series.			
SOW Annex-A	[SRS-5-26]	The IEG-C SHALL be compliant with the ISO 9241 standard series. In particular:			
SOW Annex-A	[SRS-5-27]	The IEG-C SHALL be compliant to ISO 9241-125:2017 for the presentation of information.			
SOW Annex-A	[SRS-5-28]	The IEG-C SHALL be compliant to ISO 9241-13 for user guidance.			
SOW Annex-A	[SRS-5-29]	The IEG-C SHALL be compliant to ISO 9241-14 for menu dialogues.			
SOW Annex-A	[SRS-5-3]	The IEG-C SHALL be designed to allow future scalability.			
SOW Annex-A	[SRS-5-30]	reserved			
SOW Annex-A	[SRS-5-300]	The IEG-C SHALL meet at a minimum the throughput levels defined for the individual data types shown Table 6 .			
SOW Annex-A	[SRS-5-301]	The IEG-C SHALL meet the minimum required throughput defined in Table 6, for at least 99.5% of its Operational time.			
SOW Annex-A	[SRS-5-302]	reserved			
SOW Annex-A	[SRS-5-303]	The Platform SHALL be able to support a throughput increase of 10% every year for a period of 5 years with no degradation of the maximum latency.			
SOW Annex-A	[SRS-5-304]	The IEG-C SHALL exhibit a Mean-Time-Between-Failure (MTBF) characteristic of at least 8760 operational hours.			
SOW Annex-A	[SRS-5-305]	The IEG-C SHALL implement Identity and Access Management (IAM) according to the requirements on IAM as specified in the Technical and Implementation Directive on CIS Security [NAC AC/322-D/0048-REV3, 2019].			
SOW Annex-A	[SRS-5-306]	In support of the authentication and authorization of users, the IEG-C and its sub-components SHALL support authentication and authorization based on the RADIUS protocol [IETF RFC 2865, 2000].			
SOW Annex-A	[SRS-5-308]	The IEG-C SHALL implement multifactor user authentication in accordance with in the Technical and Implementation Directive on CIS Security [NAC AC/322-D/0048-REV3, 2019].			
SOW Annex-A	[SRS-5-309]	The implementation of multifactor authentication by the IEG-C SHALL integrate with the multifactor authentication solution as it is in use in the NATO Enterprise.			
SOW Annex-A	[SRS-5-31]	The IEG-C SHALL be compliant to ISO 9241-143 for form filling dialogues			
SOW Annex-A	[SRS-5-310]	The WG System Administrator address SHALL be configurable.			
SOW Annex-A	[SRS-5-311]	The information contained in Table 6 SHALL be used to define key performance indicators (KPIs) for 'Availability', 'Quality' and 'Usage', as defined in [NCIA SMC TA, 2018].			
SOW Annex-A	[SRS-5-318]	The IEG-C, as a system, SHALL have an availability of 99.95%.			
SOW Annex-A	[SRS-5-319]	Upon restoration of services, the IEG-C Servers SHALL become fully operational.			
SOW Annex-A	[SRS-5-32]	The IEG-C SHALL be compliant to ISO 9241-171 for accessibility.			
SOW Annex-A	[SRS-5-320]	Any IEG-C component SHALL not exceed 20kg. If it is determined (by analysis and/or empirically) that this is not feasible, any deviation request shall be submitted to Purchaser approval.			
SOW Annex-A	[SRS-5-321]	Any IEG-C component using forced airflow (fan) cooling SHALL be of front-rear type.			
SOW Annex-A	[SRS-5-322]	All IEG-C component SHALL have dual power supply module. If it is determined (by analysis and/or empirically) that this is not feasible, any deviation request shall be submitted to Purchaser approval.			
SOW Annex-A	[SRS-5-323]	The IEG-C SHALL be configurable from scratch using the DCIS orchestration and automation toolset.			
SOW Annex-A	[SRS-5-324]	The IEG-C SHALL include an NSAB/NOS endorsed quick erase feature allowing the complete erasure of all configuration, stored data and software.			
SOW Annex-A	[SRS-5-325]	The quick erase feature SHALL not take longer than 30 minutes.			
SOW Annex-A	[SRS-5-326]	The quick erase feature SHALL not erase IEG-C backups.			
SOW Annex-A	[SRS-5-327]	The IEG-C backups SHALL be stored on the domain Disaster Recovery System (DRS) or, if the domain DRS is not available, a removable, local backup device.			
SOW Annex-A	[SRS-5-328]	The MG SHALL be dimensioned and configured to be able to scale in performance and support the following per year, for three years, without degradation of performance as specified in section 5.4.1.2: • a 100% increase in the SCNL (normal load for each SMTP message size category); • a 50% increase in message size.			
SOW Annex-A	[SRS-5-329]	The IEG-C as a system SHALL support the use of multiple instances in parallel, providing same gateway services between identical Low and High domains and being operated in different physical locations			
SOW Annex-A	[SRS-5-330]	When multiple IEG-C are operated in parallel between identical Low and High domains, it SHALL be possible to identify per information flow, which IEG-C acts as the primary gateway and those which act as alternates			
SOW Annex-A	[SRS-5-331]	The fall back mechanism SHALL support a seamless transition from the primary IEG-C to an alternate IEG-C for users and system administrators			
SOW Annex-A	[SRS-5-332]	It SHALL be possible to identify on the monitoring system which IEG-C (primary or alternate) is currently servicing each of the information flows			
SOW Annex-A	[SRS-5-333]	The IEG-C SHALL be able to operate 72 hours in total isolation from any central management and monitoring system			
SOW Annex-A	[SRS-5-334]	The IEG-C local backup dedicated hardware SHALL be removable in no more than 5 minutes, SHALL not exceed 5kg in weight and SHALL not exceed 30cmx30cmx30cm (Height, Wide, Deep).			
SOW Annex-A	[SRS-5-33]	The IEG-C SHALL follow the dialogue principles stated in ISO 9241-110.			

SOW Annex-A	[SRS-5-34]	In applications where users must log-on to the system, log-on SHALL be a separate procedure that must be completed before a user is required to select among any operational options.			
SOW Annex-A	[SRS-5-35]	Appropriate prompts for log-on SHOULD be automatically displayed on the user's terminal when accessing the application.			
SOW Annex-A	[SRS-5-36]	User identification procedures SHALL be as simple as possible, consistent with adequate data protection.			
SOW Annex-A	[SRS-5-37]	When required, the password SHALL not be echoed on the display. An asterisk (*) or similar symbol will be displayed for each character when inputting secure passwords during log-on.			
SOW Annex-A	[SRS-5-38]	Users SHALL be provided feedback relevant to the log-on procedure that indicates the status of the inputs.			
SOW Annex-A	[SRS-5-39]	If a user cannot log-on to a system, a prompt SHOULD be provided to explain the reason for this inability. Log-on processes SHOULD require minimum input from the user consistent with the requirements prohibiting illegal entry.			
SOW Annex-A	[SRS-5-4]	The IEG-C SHALL be expandable and scalable in performance (throughput and bandwidth).			
SOW Annex-A	[SRS-5-40]	When a user signals for system log-off, or application exit or shut-down, the system SHOULD check pending transactions to determine if data loss seems probable. If so, the computer SHOULD prompt for confirmation before the log-off command is executed.			
SOW Annex-A	[SRS-5-41]	The IEG-C SHALL be available in operational HQs, static and deployed, 24 hours a day, 7 days a week, with an availability rate of 99.5 %.			
SOW Annex-A	[SRS-5-42]	The IEG-C, including hardware, infrastructure and Operational Software, SHALL be available for use at static sites (via Data Centres) 24 hours per day, 365 days per year with an availability of 99.9% (Level 2 of Operational Continuity).			
SOW Annex-A	[SRS-5-43]	The IEG-C SHALL, despite the presence of hardware or software faults in part of the IEG-C, continue to perform the unaffected IEG-C functions.			
SOW Annex-A	[SRS-5-44]	The IEG-C Servers SHALL gracefully degrade in the condition where any dependent services and components are not available and notify the user of the limited functionality.			
SOW Annex-A	[SRS-5-46]	The IEG-C SHALL provide a rate of fault occurrence of less than 2 failures for 1000 hours of operation in the IEG-C software components, with 95% confidence. A failure is defined as an error or cessation in the operation of the software requiring, as a minimum, a restart of the software (for example, a service) to recover.			
SOW Annex-A	[SRS-5-47]	It SHALL be possible to correct any individual fault within the IEG-C within a period of time no greater than sixty (60) minutes.			
SOW Annex-A	[SRS-5-48]	The IEG-C SHALL exhibit a mean-time-between-failure (MTBF) characteristic of less than 2 failures every 7000 hours, and that SHALL not be affected by the total number of IEG-C instances which are active during that period. The MTBF measurement SHALL not include failures resulting from factors determined to be external to the IEG-C (e.g., loss of domain controller).			
SOW Annex-A	[SRS-5-49]	Reserved			
SOW Annex-A	[SRS-5-5]	The IEG-C SHALL be capable of accommodating additional functionality the need for which may arise as well as future technological improvements.			
SOW Annex-A	[SRS-5-50]	The IEG-C SHALL provide authorised users with the ability to perform full and/or incremental backups of the system's data and software without impacting system availability.			
SOW Annex-A	[SRS-5-507]	A MG System Administrator SHALL be able to successfully deploy (i.e., install and configure) the MG within a time frame of one (1) working day after receiving a maximum of five (5) days of training.			
SOW Annex-A	[SRS-5-51]	The IEG-C SHALL maintain full functionality and performance in the event of power failure(s) for a minimum of twenty (20) minutes, prior to initiating a graceful system shutdown.			
SOW Annex-A	[SRS-5-52]	In case of a failure in the power supply to the IEG-C UPS, the IEG-C SHALL react at 50% battery level with a warning and at 30% battery level with going into graceful system shutdown..			
SOW Annex-A	[SRS-5-53]	After going into graceful system shutdown caused by a power failure, the IEG-C SHALL have retained all the relevant data.			
SOW Annex-A	[SRS-5-54]	The IEG-C SHALL provide automatic resumption of operation after power restoration, except where this violates security requirements.			
SOW Annex-A	[SRS-5-55]	The IEG-C SHALL queue pending asynchronous (i.e. do not need immediate feedback) requests to an unavailable service and deliver them when the service becomes available again.			
SOW Annex-A	[SRS-5-56]	The IEG-C SHALL provide a Mean Time To Repair (MTTR) after the failure of a critical component of four (4) hours or less.			
SOW Annex-A	[SRS-5-57]	The IEG-C SHALL provide a maximum time to restore the service after the failure of a critical component of no greater than six (6) hours at the 95% confidence level.			
SOW Annex-A	[SRS-5-58]	The IEG-C SHALL provide a Time-To-Repair (TTR) of no greater than eight (8) hours for servers and their components at 100% confidence level.			
SOW Annex-A	[SRS-5-59]	In case of IEG-C failure the availability interruption SHALL not exceed two hours.			
SOW Annex-A	[SRS-5-6]	The IEG-C SHALL use an architecture that allows horizontal scalability and allows the same component to be deployed on multiple machines supporting the information exchange requirements in concert.			
SOW Annex-A	[SRS-5-60]	The IEG-C SHALL resume/retry IEG-C services in case of high latency/timeout/loss of network connectivity without loss of data. High latency is defined as latency exceeding one (1) minute.			
SOW Annex-A	[SRS-5-61]	The IEG-C SHALL provide a Mean Time Between Maintenance (MTBM) for individual components of greater than six thousand (6000) hours of continuous operation where the required maintenance action excludes restart of the hardware and software.			
SOW Annex-A	[SRS-5-62]	The IEG-C SHALL provide a MTBM of greater than thousand (1000) hours of continuous operation where the required maintenance action is only a restart of the hardware or software.			
SOW Annex-A	[SRS-5-63]	The IEG-C SHALL comply with security settings, installation guides and configuration guidelines listed in the latest approved version of the NCIA CSSL Security Configuration Catalogue.			
SOW Annex-A	[SRS-5-64]	The IEG-C components SHALL be configured with the latest security patches and updated with the latest security guidelines from the NATO Information Assurance Technical Centre (NIATC).			
SOW Annex-A	[SRS-5-65]	The IEG-C SHALL be capable of operating within the NS and MS WAN environment (including servers, network, services and workstations) in the presence of the currently approved NATO Security Settings (target version to be provided by the Purchaser during the Design Stage). Any deviations from the approved security settings SHALL be identified by the Contractor prior to testing and SHALL be subject to approval of the Purchaser.			
SOW Annex-A	[SRS-5-66]	The IEG-C SHALL uniquely Identify and Authenticate Users.			
SOW Annex-A	[SRS-5-67]	The IEG-C SHALL allow an IEG-C Administrator to manage (create, update, delete) IEG-C User Accounts, password details, and assign User Roles to User Account and manage general access privileges of individual User Accounts.			
SOW Annex-A	[SRS-5-68]	The IEG-C SHALL support the application of a password policy.			
SOW Annex-A	[SRS-5-69]	The IEG-C SHALL be configurable to deny the re-use of a specified previous passwords.			
SOW Annex-A	[SRS-5-7]	In order to keep meeting the requirements on Time Behaviour in 5.2.1.1 it SHALL be possible to apply horizontal scalability without disrupting the services offered by the IEG-C.			
SOW Annex-A	[SRS-5-70]	IEG-C SHALL be configurable to lock user accounts after a specified number of unsuccessful authentication attempts.			
SOW Annex-A	[SRS-5-71]	IEG-C passwords SHALL be stored in encrypted form.			
SOW Annex-A	[SRS-5-72]	IEG-C SHALL support the locking of accounts that are no longer required for a specified period of time after which they SHALL be deleted.			
SOW Annex-A	[SRS-5-73]	The IEG-C SHALL support the protection of User credentials in transit.			
SOW Annex-A	[SRS-5-74]	The IEG-C SHALL provide privileged IEG-C accounts (e.g., system and security administrator accounts).			
SOW Annex-A	[SRS-5-75]	The IEG-C SHALL allow authenticated Users to manage their password.			
SOW Annex-A	[SRS-5-76]	The IEG-C SHALL generate audit records for auditable events, addressing, among others, the following events: • system start-up (including re-starts) and shutdown; • log-on (including log-on attempts) and log-off of individual users • changes to permissions and privileges of users and groups; • changes to security relevant system management information(including audit functions); • start-up and shutdown of the audit function; • any access to security data; • deletion, creation or alteration of the security audit records; • changes to system date and time; • unsuccessful attempts to access system resources;			
SOW Annex-A	[SRS-5-77]	Audit tracing in the IEG-C SHALL be permanently effective.			
SOW Annex-A	[SRS-5-78]	The IEG-C SHALL protect the information from unauthorised modification or deletion.			
SOW Annex-A	[SRS-5-79]	The IEG-C SHALL establish access permissions to audit information.			
SOW Annex-A	[SRS-5-80]	The IEG-C SHALL associate individual user identities to auditable events in the event log.			
SOW Annex-A	[SRS-5-81]	The IEG-C SHALL include the date and time of each auditable event in the event log.			
SOW Annex-A	[SRS-5-82]	The IEG-C SHALL alert an IEG-C Administrator on failed attempts at log-on.			
SOW Annex-A	[SRS-5-83]	The IEG-C SHALL create and maintain an archive of audit information.			
SOW Annex-A	[SRS-5-84]	The IEG-C SHALL support the retaining of audit information for a specified period of time.			
SOW Annex-A	[SRS-5-85]	The IEG-C SHALL record in traceable logs all selected transactions, database activities, technical events (e.g., dataset synchronisation, directory replication) and accessing of data.			
SOW Annex-A	[SRS-5-86]	If so configured, the IEG-C SHALL log all configurations changes with the trace to persons or systems.			

SOW Annex-A	[SRS-5-87]	The IEG-C SHALL generate and maintain an Audit Log for each of the following auditable events, SHALL associate individual User identities to those events, and SHALL include date and time of the event, type of event, User identity, and the outcome (success or failure) of the event: • System start-up and shutdown, • the start/end time of usage of system applications (system components) by individual Users • Changes to permissions and privileges of Users and groups, • Changes to security relevant system management function, • Configuration changes, • Any access to audit log, • Deletion, creation or alteration of the security audit records, • All privileged operations, • All updates of IEG-C access rights, • All attempts to delete, write or append the Audit files.			
SOW Annex-A	[SRS-5-88]	The IEG-C SHALL use integrity checking countermeasures to ensure that the Audit Log has been archived successfully.			
SOW Annex-A	[SRS-5-89]	The IEG-C SHALL support the following warning system events based on configurable limits: • Network bandwidth low; • Percentage of disk space left; • Percentage of table space left.			
SOW Annex-A	[SRS-5-9]	The IEG-C SHALL be Vertical Scalable, i.e. IEG-C SHALL be able to adapt its performance characteristics by adding additional system resources such as processing power, memory, disk capacity, or network capacity.			
SOW Annex-A	[SRS-5-90]	Sessions SHALL be invalidated when the user logs out.			
SOW Annex-A	[SRS-5-91]	Sessions SHALL timeout after a specified period of inactivity.			
SOW Annex-A	[SRS-5-92]	The runtime environment or parser SHALL not be susceptible to XML and XPath injection.			
SOW Annex-A	[SRS-5-93]	The IEG-C SHALL have defences against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, environment, etc.)			
SOW Annex-A	[SRS-5-94]	Sensitive data SHALL be sanitized from memory as soon as it is no longer needed.			
SOW Annex-A	[SRS-5-95]	A certificate path SHALL be built and validated from a trusted CA to each Transport Layer Security (TLS) server certificate, and each server certificate SHALL match the Fully Qualified Domain Name of the server.			
SOW Annex-A	[SRS-5-96]	Failed TLS connections SHALL not fall back to an insecure connection.			
SOW Annex-A	[SRS-5-97]	Certificate paths SHALL be built and validated for all client certificates using configured trust anchors and revocation information.			
SOW Annex-A	[SRS-5-98]	The application logic SHALL have protection mechanisms against application crashing, memory access violations (buffer overflow) and unexpected exceptions such as data destruction and resource depletion (Memory, CPU, Bandwidth, Disk Space, etc.).			
SOW Annex-A	[SRS-5-99]	The application SHALL have sufficient access controls to prevent elevation of privilege attacks.			
SOW Annex-A	[SRS-6-1]	The WG MUST provide a data exchange capability WG_DEX that facilitates the mediation of data between the high domain and the low domain.			
SOW Annex-A	[SRS-6-10]	WG_IF_MGMT MUST support an operation 'ReceiveManagement' that receives data from the management domain for processing by the WG.			
SOW Annex-A	[SRS-6-100]	For every action taken, the operation 'Enforce LH SOA Platform IFCPE' SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the action.			
SOW Annex-A	[SRS-6-101]	If WG_IFP_SOA_LH does not permit the release of information due to a policy violation, the WG SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the outcome O_WG_IFCPE ([SRS-6-115]).			
SOW Annex-A	[SRS-6-102]	The WG SHALL ensure that no illicit information flows exist to circumvent the enforcement of WG_IFP_SOA_LH.			
SOW Annex-A	[SRS-6-103]	For incoming and outgoing management traffic at WG_IF_MGMT, WG_IFCPE MUST offer an interface 'IFCPE Services Management' that accepts information for further processing.			
SOW Annex-A	[SRS-6-104]	The interface 'IFCPE Services Management' MUST support an operation 'Enforce Management Communications IFCPE' that enforces the policy WG_IFP_MGMT.			
SOW Annex-A	[SRS-6-105]	The operation 'Enforce Management Communications IFCPE' SHOULD enforce the policy WG_IFP_MGMT_IN on the following information flow: • Source: Communications Access Services Management Interface -> ReceiveNetworkManagement • Destination: Core Services Management Interface -> ReceiveManagementContent • Information: Management traffic. • Operation: pass management traffic by ensuring the following conditions: o WG_IFP_MGMT_IN permits information flow.			
SOW Annex-A	[SRS-6-106]	The operation 'Enforce Management Communications IFCPE' SHOULD enforce the policy WG_IFP_MGMT_OUT on the following information flow: • Source: Core Services Management Interface -> ForwardManagementContent • Destination: Communications Access Services Management Interface -> ForwardNetworkManagement • Information: Management traffic. • Operation: pass management traffic by ensuring the following conditions: o WG_IFP_MGMT_OUT permits information flow.			
SOW Annex-A	[SRS-6-107]	If WG_IFP_MGMT_IN or WG_IFP_MGMT_OUT do not permit information flow, the WG SHALL execute the action specified in WG_IFP_MGMT.			
SOW Annex-A	[SRS-6-108]	For every action taken, the operation 'Enforce Management Communications IFCPE' SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the action.			
SOW Annex-A	[SRS-6-109]	If WG_IFP_MGMT does not permit the release of information due to a policy violation, the WG SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the outcome O_WG_IFCPE ([SRS-6-115]).			
SOW Annex-A	[SRS-6-11]	WG_IF_MGMT MUST support an operation 'ForwardManagement' that forwards data that has been processed by the WG to the management domain.			
SOW Annex-A	[SRS-6-110]	The WG SHALL ensure that no illicit information flows exist to circumvent the enforcement of WG_IFP_MGMT.			
SOW Annex-A	[SRS-6-111]	WG_IFP SHALL be configurable.			
SOW Annex-A	[SRS-6-112]	WG_IFP SHALL specify the actions ACTIONS that need to be executed by WG_IFCPE.			
SOW Annex-A	[SRS-6-113]	For each action in ACTIONS it SHALL be possible to: • Enable or disable the action. • Instruct WG_IFCPE to ignore the outcome of the execution of the action. • If the outcome O_WG_IFCPE of the execution of the action is negative (e.g. verification or validation fails, or a policy violation was determined): instruct WG_IFCPE to continue the enforcement of WG_IFP, or to stop.			
SOW Annex-A	[SRS-6-114]	It SHALL be possible to enable or disable the enforcement of each of the following sub-policies: • WG_IFP_CA_LH_IN; • WG_IFP_CA_LH_OUT; • WG_IFP_CA_HL_IN; • WG_IFP_CA_HL_OUT; • WG_IFP_MGMT_IN; • WG_IFP_MGMT_OUT; • WG_IFP_SOA_LH; • WG_IFP_SOA_HL.			
SOW Annex-A	[SRS-6-115]	WG_IFP SHALL specify the level of granularity of the outcome O_WG_IFCPE. It SHALL be possible for WG_IFCPE to distinguish within O_WG_IFCPE: • The sub-policy ([SRS-6-114]) that was enforced when a policy violation was determined; • Identification of the action that led to the policy violation; • Reason for policy violation.			
SOW Annex-A	[SRS-6-116]	The policies WG_IFP_CA_HL, WG_IFP_CA_LH and WG_IFP_MGMT SHALL specify: • That an information flow (as described in 6.5.1.2.2, 6.5.1.3.2 and 6.5.1.4.2 respectively) is not permitted if the outcome O_WG_IFCPE constitutes a policy violation; • The action the WG shall take in case information flow is not permitted. The possible actions SHALL include: o Silently drop traffic; o Reset the TCP/IP connection.			
SOW Annex-A	[SRS-6-117]	The policy WG_IFP_CA_HL_IN SHALL specify the actions ACTIONS_WG_CA_HL_IN that the operation 'Enforce HL Communications IFCPE' SHALL execute for the information flow described in ([SRS-6-74]).			
SOW Annex-A	[SRS-6-118]	ACTIONS_WG_CA_HL_IN SHALL include the following actions: • Filter traffic based on the ruleset RULESET_WG_IFCPE-CA_HL_IN.			
SOW Annex-A	[SRS-6-119]	The policy WG_IFP_CA_HL_OUT SHALL specify the actions ACTIONS_WG_CA_HL_OUT that the operation 'Enforce HL Communications IFCPE' SHALL execute for the information flow described in ([SRS-6-75]).			
SOW Annex-A	[SRS-6-12]	WG_DEX MUST offer a TCP/IP [IETF RFC 791, 1981], [IETF RFC 2460, 1998], [IETF RFC 7414, 2015] over Ethernet interface 'Communications Access Services HL' on top of WG_IF_NET_HIGH and WG_IF_NET_LOW.			
SOW Annex-A	[SRS-6-120]	ACTIONS_WG_CA_HL_OUT SHALL include the following actions: • Filter traffic based on the ruleset RULESET_WG_IFCPE-CA_HL_OUT.			
SOW Annex-A	[SRS-6-121]	The policy WG_IFP_CA_LH_IN SHALL specify the actions ACTIONS_WG_CA_LH_IN that the operation 'Enforce LH Communications IFCPE' SHALL execute for the information flow described in ([SRS-6-89]).			
SOW Annex-A	[SRS-6-122]	ACTIONS_WG_CA_LH_IN SHALL include the following actions: • Filter traffic based on the ruleset RULESET_WG_IFCPE-CA_LH_IN.			
SOW Annex-A	[SRS-6-123]	The policy WG_IFP_CA_LH_OUT SHALL specify the actions ACTIONS_WG_CA_LH_OUT that the operation 'Enforce LH Communications IFCPE' SHALL execute for the information flow described in ([SRS-6-90]).			

SOW Annex-A	[SRS-6-124]	ACTIONS_WG_CA_LH_OUT SHALL include the following actions: • Filter traffic based on the ruleset RULESET_WG_IFCPE-CA_LH_OUT.			
SOW Annex-A	[SRS-6-125]	The policy WG_IFP_MGMT_IN SHALL specify the actions ACTIONS_WG_MGMT_IN that the operation 'Enforce Management Communications IFCPE' SHALL execute for the information flow described in [SRS-6-105].			
SOW Annex-A	[SRS-6-126]	ACTIONS_WG_MGMT_IN SHALL include the following actions: • Filter traffic based on the ruleset RULESET_WG_IFCPE-MGT_IN.			
SOW Annex-A	[SRS-6-127]	The policy WG_IFP_MGMT_OUT SHALL specify the actions ACTIONS_WG_MGMT_OUT that the operation 'Enforce Management Communications IFCPE' SHALL execute for the information flow described in [SRS-6-106].			
SOW Annex-A	[SRS-6-128]	ACTIONS_WG_MGMT_OUT SHALL include the following actions: • Filter traffic based on the ruleset RULESET_WG_IFCPE-MGT_OUT.			
SOW Annex-A	[SRS-6-129]	The policy WG_IFP_CA_HL SHALL specify RULESET_WG_IFCPE-CA_HL_IN and RULESET_WG_IFCPE-CA_HL_OUT.			
SOW Annex-A	[SRS-6-13]	The interface 'Communications Access Services HL' MUST support an operation 'ReceiveInternalNetworkHL' on top of WG_IF_NET_HIGH that provides TCP/IP connectivity on the high domain by receiving IP traffic for processing by the WG.			
SOW Annex-A	[SRS-6-130]	RULESET_WG_IFCPE-CA_HL_IN and RULESET_WG_IFCPE-CA_HL_OUT SHALL be configurable.			
SOW Annex-A	[SRS-6-131]	The policy WG_IFP_CA_LH SHALL specify RULESET_WG_IFCPE-CA_LH_IN and RULESET_WG_IFCPE-CA_LH_OUT.			
SOW Annex-A	[SRS-6-132]	RULESET_WG_IFCPE-CA_LH_IN and RULESET_WG_IFCPE-CA_LH_OUT SHALL be configurable.			
SOW Annex-A	[SRS-6-133]	The policy WG_IFP_MGMT SHALL specify RULESET_WG_IFCPE-MGT_IN and RULESET_WG_IFCPE-MGT_OUT.			
SOW Annex-A	[SRS-6-134]	RULESET_WG_IFCPE-MGT_IN and RULESET_WG_IFCPE-MGT_OUT SHALL be configurable.			
SOW Annex-A	[SRS-6-135]	Each of the rulesets RULESET_WG_IFCPE-CA_HL_IN, RULESET_WG_IFCPE-CA_HL_OUT, RULESET_WG_IFCPE-CA_LH_IN, RULESET_WG_IFCPE-CA_LH_OUT, RULESET_WG_IFCPE-MGT_IN, RULESET_WG_IFCPE-MGT_OUT SHALL include: • Identification of traffic flow that is allowed or disallowed based on source and destination IP addresses; • Identification of traffic that is allowed or disallowed based on protocols and ports; • Identification of traffic that is allowed or disallowed based on values of protocol fields.			
SOW Annex-A	[SRS-6-136]	The policy WG_IFP_SOA_HL SHALL specify: • That a release of information to the low domain is not permitted if O_WG_CIPE_HL ([SRS-6-148]) constitutes a policy violation; • The action the WG shall take in case of a policy violation, see [SRS-6-138].			
SOW Annex-A	[SRS-6-137]	The policy WG_IFP_SOA_LH SHALL specify: • That an import of information to the high domain is not permitted if O_WG_CIPE_LH ([SRS-6-155]) constitutes a policy violation; • The action the WG shall take in case of a policy violation, see [SRS-6-138].			
SOW Annex-A	[SRS-6-138]	The policies WG_IFP_SOA_HL and WG_IFP_SOA_LH SHALL specify the action the WG shall take in case of a policy violation. The possible actions SHALL include: • Silently drop traffic; • Send an HTTP error response of a specific type; o The type of HTTP error message SHALL be configurable. • Send a custom HTTP error message; o The contents of the custom HTTP error message SHALL be configurable. o It SHALL be possible to include the items in [SRS-6-163].			
SOW Annex-A	[SRS-6-139]	The WG MUST provide a content inspection policy enforcement (CIPE) capability WG_CIPE that enables the WG to manage and schedule the routing of content through content filters (by WG_CIS ([SRS-6-190])) in accordance with the WG content inspection policy WG_CIP.			
SOW Annex-A	[SRS-6-14]	The operation 'ReceiveInternalNetworkHL' MUST support error handling as specified in [IETF RFC 7414, 2015].			
SOW Annex-A	[SRS-6-140]	The design and functionality of WG_CIPE SHOULD conform to the NATO CIPE functional specification in [NC3A TN-1486, 2012].			
SOW Annex-A	[SRS-6-395]	If WG_CIPE does not conform to the NATO CIPE functional specification in [NC3A TN-1486, 2012], the proposed functional specification of the WG_CIPE SHALL be de-scribed in the bid response.			
SOW Annex-A	[SRS-6-397]	The WG_CIPE SHALL be able to be configured to support the “Content Inspection Policy Enforcement Profile for a Medium Assurance NATO XML-Labelling Guard” [NC3A TR/2012/SPW007959/03].			
SOW Annex-A	[SRS-6-141]	WG_CIPE SHALL ensure that no illicit information flows exist to circumvent the enforcement of WG_CIP.			
SOW Annex-A	[SRS-6-142]	WG_CIPE SHALL ensure that enforcement actions are executed in the order as specified in WG_CIP ([SRS-6-159]).			
SOW Annex-A	[SRS-6-143]	For the flow of information from WG_IF_NET_HIGH to WG_IF_NET_LOW, WG_CIPE MUST offer an interface 'CIPE Services High to Low' that accepts information for further processing.			
SOW Annex-A	[SRS-6-144]	The interface 'CIPE Services High to Low' MUST support an operation 'Enforce HL SOA CIPE' that enforces the policy WG_CIP_HL.			
SOW Annex-A	[SRS-6-145]	The operation 'Enforce HL SOA CIPE' MUST support the invocation of the following operations at the interface 'Content Inspection Services' ([SRS-6-194]) provided by WG_CIS ([SRS-6-190]): • Operation ‘Initialize’ ([SRS-6-199]) that takes as input an identifier CIPE_CF_ID that identifies a content filter in WG_CIS; • Operation ‘Filter’ ([SRS-6-201]) that takes as input a data object CIPE_DATA and a set of rules CIPE_DATA_RULES for processing CIPE_DATA; • Operation ‘Halt’ ([SRS-6-203]) that takes as input an attribute CIPE_CF_ID that identifies a content filter in WG_CIS.			
SOW Annex-A	[SRS-6-146]	WG_CIPE SHALL determine CIPE_CF_ID, CIPE_DATA and CIPE_DATA_RULES based on the policy WG_CIP_HL.			
SOW Annex-A	[SRS-6-147]	For every action taken, the operation 'Enforce HL SOA CIPE' SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the action.			
SOW Annex-A	[SRS-6-148]	WG_CIPE SHALL inform WG_IFCPE of the outcome O_WG_CIPE_HL of the enforcement of WG_CIP_HL based on WG_CIP ([SRS-6-163]).			
SOW Annex-A	[SRS-6-149]	WG_CIPE SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log O_WG_CIPE_HL.			
SOW Annex-A	[SRS-6-15]	The interface 'Communications Access Services HL' MUST support an operation 'ForwardInternalNetworkHL' on top of WG_IF_NET_LOW that forwards IP traffic to the low domain.			
SOW Annex-A	[SRS-6-150]	For the flow of information from WG_IF_NET_LOW to WG_IF_NET_HIGH, WG_CIPE MUST offer an interface 'CIPE Services Low to High' that accepts information for further processing.			
SOW Annex-A	[SRS-6-151]	The interface 'CIPE Services Low to High' MUST support an operation 'Enforce LH SOA CIPE' that enforces the policy WG_CIP_LH.			
SOW Annex-A	[SRS-6-152]	The operation 'Enforce LH SOA CIPE' MUST support the invocation of the following operations at the interface 'Content Inspection Services' ([SRS-6-194]) provided by WG_CIS ([SRS-6-190]): • Operation ‘Initialize’ ([SRS-6-199]) that takes as input an identifier CIPE_CF_ID that identifies a content filter in WG_CIS; • Operation ‘Filter’ ([SRS-6-201]) that takes as input a data object CIPE_DATA and a set of rules CIPE_DATA_RULES for processing CIPE_DATA; • Operation ‘Halt’ ([SRS-6-203]) that takes as input an attribute CIPE_CF_ID that identifies a content filter in WG_CIS.			
SOW Annex-A	[SRS-6-153]	reserved			
SOW Annex-A	[SRS-6-154]	For every action taken, the operation 'Enforce LH SOA CIPE' SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the action.			
SOW Annex-A	[SRS-6-155]	WG_CIPE SHALL inform WG_IFCPE of the outcome O_WG_CIPE_LH of the enforcement of WG_CIP_LH based on WG_CIP ([SRS-6-163]).			
SOW Annex-A	[SRS-6-156]	WG_CIPE SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log O_WG_CIPE_LH.			
SOW Annex-A	[SRS-6-157]	WG_CIP SHALL be configurable.			
SOW Annex-A	[SRS-6-158]	WG_CIP SHALL specify the actions ACTIONS that need to be executed by WG_CIS.			
SOW Annex-A	[SRS-6-159]	WG_CIP SHALL specify the order in which ACTIONS need to be executed.			
SOW Annex-A	[SRS-6-16]	The operation 'ForwardInternalNetworkHL' MUST support error handling as specified in [IETF RFC 7414, 2015].			
SOW Annex-A	[SRS-6-160]	For each action in ACTIONS it SHALL be possible to: • Enable or disable the action. • Instruct WG_CIPE to ignore the outcome of the execution of the action by WG_CIS (as received from WG_CIS ([SRS-6-206])). • If the outcome of the execution of the action by WG_CIS is a policy violation: instruct WG_CIPE to continue the enforcement of WG_CIP, or to stop.			
SOW Annex-A	[SRS-6-161]	It SHALL be possible to group ACTIONS per the following sub-policies: • WG_CIP_LH_SV; • WG_CIP_LH_HV; • WG_CIP_LH_MD; • WG_CIP_HL_HV; • WG_CIP_HL_LV.			
SOW Annex-A	[SRS-6-162]	It SHALL be possible to enable or disable the enforcement of each sub-policy in ([SRS-6-161]).			
SOW Annex-A	[SRS-6-163]	WG_CIP SHALL specify the level of granularity of the outcomes O_WG_CIS ([SRS-6-205]), O_WG_CIPE_HL ([SRS-6-148]) and O_WG_CIPE_LH ([SRS-6-155]). It SHALL be possible for WG_CIS to distinguish within O_WG_CIS, O_WG_CIPE_HL and O_WG_CIPE_LH: • The WG_CIS capability that determined a policy violation (WG_CIS_SV ([SRS-6-208]), WG_CIS_HV ([SRS-6-213]), WG_CIS_LV ([SRS-6-219]), and WG_CIS_MD ([SRS-6-508]); • Identification CIPE_CF_ID of the content filter that determined the policy violation; • Identification of the action that led to policy violation; • Reason for policy violation.			
SOW Annex-A	[SRS-6-164]	The policy WG_CIP_LH_SV SHALL specify the actions ACTIONS_WG_LH_SV that need to be performed by WG_CIS_SV.			
SOW Annex-A	[SRS-6-165]	ACTIONS_WG_LH_SV SHALL include the following actions: • Check the HTTP message body for XML well-formedness; • Validate the HTTP message body against a list of W3C XML Schemas LIST_WG_CIS_SV-XS; o Select LIST_WG_CIS_SV-XS based on the URI in the HTTP message startline. • Check that the namespace of the root node belongs to a list of allowed namespaces LIST_WG_CIS_SV-NS; o Select LIST_WG_CIS_SV-NS based on the URI in the HTTP message startline.			
SOW Annex-A	[SRS-6-166]	WG_CIP_LH_SV SHALL specify LIST_WG_CIS_SV-XS.			

SOW Annex-A	[SRS-6-167]	LIST_WG_CIS_SV-XS SHALL be configurable.			
SOW Annex-A	[SRS-6-168]	WG_CIP_LH_SV SHALL include the option to specify a LIST_WG_CIS_SV-XS for a given URI.			
SOW Annex-A	[SRS-6-169]	WG_CIP_LH_SV SHALL specify LIST_WG_CIS_SV-NS.			
SOW Annex-A	[SRS-6-17]	WG_DEX MUST offer a TCP/IP [IETF RFC 791, 1981], [IETF RFC 2460, 1998], [IETF RFC 7414, 2015] over Ethernet interface 'Communications Access Services LH' on top of WG_IF_NET_LOW and WG_IF_NET_HIGH.			
SOW Annex-A	[SRS-6-170]	LIST_WG_CIS_SV-NS SHALL be configurable.			
SOW Annex-A	[SRS-6-171]	WG_CIP_LH_SV SHALL include the option to specify a LIST_WG_CIS_SV-NS for a given URI.			
SOW Annex-A	[SRS-6-172]	The policy WG_CIP_HL_HV SHALL specify the actions ACTIONS_WG_HL_HV that need to be performed by WG_CIS_HV.			
SOW Annex-A	[SRS-6-173]	ACTIONS_WG_HL_HV SHALL include the following actions based on RULESET_WG_CIS_HV-HL: • Verify the information attributes in [SRS-6-214] ; • Add or rewrite a header line; • Remove a header line; • Add or rewrite a value; • Remove a value; • Translate a URI to another value; • Normalize the URIs in header lines of an HTTP message (i.e. remove all unneeded or escaped characters from a URI and ensure sure all characters that require escaping are escaped).			
SOW Annex-A	[SRS-6-174]	WG_CIP_HL_HV SHALL specify RULESET_WG_CIS_HV-HL.			
SOW Annex-A	[SRS-6-175]	RULESET_WG_CIS_HV-HL SHALL be configurable.			
SOW Annex-A	[SRS-6-176]	The policy WG_CIP_LH_HV SHALL specify the actions ACTIONS_WG_LH_HV that need to be performed by WG_CIS_HV.			
SOW Annex-A	[SRS-6-177]	ACTIONS_WG_LH_HV SHALL include the following actions based on RULESET_WG_CIS_HV-LH: • Verify the information attributes in [SRS-6-214] ; • Add or rewrite a header line; • Remove a header line; • Add or rewrite a value; • Remove a value; • Translate a URI to another value; • Normalize the URIs in header lines of an HTTP message (i.e. remove all unneeded or escaped characters from a URI and ensure sure all characters that require escaping are escaped).			
SOW Annex-A	[SRS-6-178]	WG_CIP_LH_HV SHALL specify RULESET_WG_CIS_HV-LH.			
SOW Annex-A	[SRS-6-179]	RULESET_WG_CIS_HV-LH SHALL be configurable.			
SOW Annex-A	[SRS-6-18]	The interface 'Communications Access Services LH' MUST support an operation 'ReceiveInternalNetworkLH' on top of WG_IF_NET_LOW that provides TCP/IP connectivity on the low domain by receiving IP traffic for processing by the WG.			
SOW Annex-A	[SRS-6-180]	Each of the rulesets RULESET_WG_CIS_HV-HL and RULESET_WG_CIS_HV-LH SHALL include: • Whitelist of allowed values for the information attributes in [SRS-6-214] ; • Whitelist of allowed header lines; • Header lines that shall be present in the message header; • Header lines that shall not be present in the message header; • Rules on the start line: o Format MUST be according to [IETF RFC 7230, 2014], or [IETF RFC 7540, 2014], depending on the version; o Allowed values for the scheme; o Allowed values for HTTP version; o All case-insensitive parts MUST be lowercase; o Maximum length of URI; o Maximum number of arguments in URI; o Whitelist of allowed URIs; o Value to translate a given URI to; o Unneeded whitespace SHALL not be present; o Allowed values for 'Status Codes; o Allowed values for 'Reason String''. • Rules on the header lines: o Remove headers that are not on the whitelist; o Remove values that are not on the whitelist; o Values that must be added (or rewritten) if not present; o Value to translate a given URI to; o Maximum length of header; o Whitelist of allowed character sets; o All case-insensitive parts MUST be lowercase; o Host header line: MUST match hostname in start-line URI; o Content-Length header line: value MUST be correct.			
SOW Annex-A	[SRS-6-181]	The policy WG_CIP_HL_LV SHALL specify the actions ACTIONS_WG_HL_LV that need to be performed by WG_CIS_LV.			
SOW Annex-A	[SRS-6-182]	ACTIONS_WG_HL_LV SHALL include the following actions: • Verify that the syntax of the confidentiality metadata label conforms to ADatP-4774 "Confidentiality Metadata Label Syntax" [STANAG 4774]; • Verify that the binding mechanism used conforms to ADatP-4778 "Metadata Binding Mechanism" [STANAG 4778]; • Verify that the binding profile that is applied conforms to "XML Signature Cryptographic Artefact Profile" in [STANAG 4778 SRD.2]; • Validate the BindingInformation element (see [STANAG 4778]) against a list of W3C XML Schemas LIST_WG_CIS_LV-XS. • Verify that the value of any TransformAlgorithm attribute is allowed according to a list of allowed values LIST_WG_CIS_LV-TR as specified in [STANAG 4778 SRD.2]; • Verify that the value of any CanonicalizationMethodAlgorithm attribute is allowed according to a list of allowed values LIST_WG_CIS_LV-CM as specified in [STANAG 4778 SRD.2]; • Verify that the value of any DigestMethodAlgorithm attribute is allowed according to a list LIST_WG_CIS_LV-DM as specified in [STANAG 4778 SRD.2]; • Verify that the value of any SignatureMethodAlgorithm attribute used for a digital signature is allowed according to a list LIST_WG_CIS_LV-SM_PKI as specified in [STANAG 4778 SRD.2]; • Verify that the value of any SignatureMethodAlgorithm attribute used for a keyed-hash message authentication code (HMAC) is allowed according to a list LIST_WG_CIS_LV-SM_HMAC as specified in [STANAG 4778 SRD.2]; • Check the validity of certificates against a certificate revocation list LIST_WG_CIS_LV-CRL or by using OCSP; • Evaluate the binding according to [STANAG 4778] and [STANAG 4778 SRD.2]. Evaluation SHALL include: o Identify the complete set of data objects S that are labelled (i.e. for each data object DO in S there is a confidentiality metadata label CL identified that is bound to DO). o For each data object DO in S, associate the information attributes in ([SRS-6-233]) with DO. • For each data object DO in S, verify the values of the information attributes in ([SRS-6-233]) against a Metadata Policy Information File (MPIF) MPIF_NATO; • For each data object DO in S, verify that DO can be released to the low domain based on RULESET_WG_CIS_LV; • Sanitize the body of the HTTP message based on RULESET_WG_CIS_LV; (Note that the rule set RULESET_WG_CIS_LV will specify whether or not data sanitization shall take place.) • In the case of sanitization of a file for which a filename has been specified of the form <FILENAME.EXTENSION>, modify the filename to '<FILENAME-SANITIZED_STRING-TIMESTAMP.EXTENSION>' with 'SANITIZED_STRING' and 'TIMESTAMP' as defined in RULESET_WG_CIS_LV. • Modify Binding Information for DO based on RULESET_WG_CIS_LV.			
SOW Annex-A	[SRS-6-183]	WG_CIP_HL_LV SHALL specify the lists: • LIST_WG_CIS_LV-XS; • LIST_WG_CIS_LV-TR; • LIST_WG_CIS_LV-CM; • LIST_WG_CIS_LV-DM; • LIST_WG_CIS_LV-SM_PKI; • LIST_WG_CIS_LV-SM_HMAC; • LIST_WG_CIS_LV-CRL.			
SOW Annex-A	[SRS-6-184]	All lists in [SRS-6-183] SHALL be configurable.			
SOW Annex-A	[SRS-6-185]	WG_CIP_HL_LV SHALL specify the metadata policy information file MPIF_NATO.			
SOW Annex-A	[SRS-6-187]	WG_CIP_HL_LV SHALL specify RULESET_WG_CIS_LV.			
SOW Annex-A	[SRS-6-188]	RULESET_WG_CIS_LV SHALL be configurable.			

SOW Annex-A	[SRS-6-189]	RULESET_WG_CIS_LV SHALL specify: • The clearance level of the low domain (based on the classification level of the low domain and the clearance levels of the actors in the low domain) in accordance with [STANAG 4774]; • One or more additional (alternative) clearance levels of the low domain, if required. • The clearance level of the high domain (based on the classification level of the high domain and the clearance levels of the actors in the high domain); • One or more additional (alternative) clearance levels of the high domain, if required. • Given a data object DO to which a confidentiality metadata label CL is bound, the requirements R that the values of the information attributes in CL ([SRS-6-233]) must meet in order for DO to be releasable from the high domain to the low domain. o R SHALL be expressed in terms of values of the information attributes in CL ([SRS-6-233]) and values that comprise the clearance levels of the low and the high domain; o It SHALL be possible to express R in terms of a series of AND and OR statements. • Rules for releasing a data object for which the binding is granular (as defined in [STANAG 4778]); • Rules for releasing a data object that has an alternative confidentiality metadata label bound to it; • Whether or not a confidentiality metadata label and associated binding information for DO shall be removed before release of DO. • Whether or not signatures shall be removed before release of DO. • Whether or not data sanitization shall be applied; • If data sanitization shall be applied: o The rules for data sanitization based on the use of a granular binding; o Whether or not a confidentiality metadata label and associated binding information for DO shall be removed before release of DO. o Whether or not a confidentiality metadata label and associated binding information for DO shall be regenerated based on the sanitization of DO. • Whether or not the WG shall sign the released content. • The text string 'SANITIZED_STRING' which will be added to the filename of sanitized files. • The format of the date variable 'TIMESTAMP' based on RFC 3339 [IETF RFC 3339, 2002].			
SOW Annex-A	[SRS-6-19]	The operation 'ReceiveInternalNetworkLH' MUST support error handling as specified in [IETF RFC 7414, 2015].			
SOW Annex-A	[SRS-6-190]	The WG MUST provide a content inspection services (CIS) capability WG_CIS that enables WG_CIPE to identify, verify and transform content based on the content inspection policy WG_CIP.			
SOW Annex-A	[SRS-6-191]	For the identification, verification and transformation of content based on WG_CIP, WG_CIS SHOULD provide a content-filter capability as specified in the NATO CIPE functional specification in [NC3A TN-1486, 2012].			
SOW Annex-A	[SRS-6-396]	If WG_CIPE does not conform to the NATO CIPE functional specification in [NC3A TN-1486, 2012], the proposed functional specification of the WG_CIPE SHALL be de-scribed in the bid response.			
SOW Annex-A	[SRS-6-398]	The WG_CIPE SHALL be able to be configured to support the "Content Inspection Policy Enforcement Profile for a Medium Assurance NATO XML-Labelling Guard" [NC3A TR/2012/SPW007959/03].			
SOW Annex-A	[SRS-6-192]	WG_CIS SHALL support the message syntax of HTTP messages as defined in Hypertext Transfer Protocol - HTTP/1.1 [IETF RFC 7230, 2014].			
SOW Annex-A	[SRS-6-193]	WG_CIS SHALL support XML 1.0 [W3C XML, 2006].			
SOW Annex-A	[SRS-6-194]	WG_CIS SHALL support the XML Schema Language 1.0 [W3C XML Schema 1, 2004], [W3C XML Schema 2, 2004].			
SOW Annex-A	[SRS-6-195]	WG_CIS SHALL support Canonical XML Version 1.1 [W3X Canonical XML 1.1, 2008].			
SOW Annex-A	[SRS-6-196]	WG_CIS SHALL support XML Path Language (XPath) Version 1.0 [W3C XML Path Language 1.0, 1999].			
SOW Annex-A	[SRS-6-197]	WG_CIS SHALL support XML Pointer Language (XPointer) [W3C XPointer, 2002].			
SOW Annex-A	[SRS-6-198]	WG_CIS MUST offer an interface 'Content Inspection Services' that serves as a communication mechanism between the content filters and WG_CIPE.			
SOW Annex-A	[SRS-6-199]	The interface 'Content Inspection Services' MUST support an operation 'Initialize' that initializes a content filter.			
SOW Annex-A	[SRS-6-2]	WG_DEX MUST offer a physical network interface WG_IF_NET_HIGH that provides Ethernet connectivity to the high domain.			
SOW Annex-A	[SRS-6-20]	The interface 'Communications Access Services LH' MUST support an operation 'ForwardInternalNetworkLH' on top of WG_IF_NET_HIGH that forwards IP traffic to the high domain.			
SOW Annex-A	[SRS-6-200]	The operation 'Initialize' MUST support the identification of a content filter based on a content filter identifier CIPE_CF_ID.			
SOW Annex-A	[SRS-6-201]	The interface 'Content Inspection Services' MUST support an operation 'Filter' that executes a content filter.			
SOW Annex-A	[SRS-6-202]	The operation 'Filter' SHALL accept as input a data object CIPE_DATA and a set of rules CIPE_DATA_RULES for processing CIPE_DATA.			
SOW Annex-A	[SRS-6-203]	The interface 'Content Inspection Services' MUST support an operation 'Halt' that halts a content filter.			
SOW Annex-A	[SRS-6-204]	The operation 'Halt' MUST support the identification of a content filter based on a content filter identifier CIPE_CF_ID.			
SOW Annex-A	[SRS-6-205]	WG_CIS SHALL inform WG_CIPE of the outcome O_WG_CIS of the execution of an action in ACTIONS ([SRS-6-158]).			
SOW Annex-A	[SRS-6-206]	If the outcome O_WG_CIS is negative (e.g. verification or validation fails), WG_CIS SHALL interpret O_WG_CIS as a policy violation and inform WG_CIPE according to WG_CIP ([SRS-6-163]).			
SOW Annex-A	[SRS-6-207]	WG_CIS SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the outcome O_WG_CIS ([SRS-6-115]).			
SOW Annex-A	[SRS-6-208]	WG_CIS SHALL provide an XML schema validation capability WG_CIS_SV that comprises the content filters that are executed in order to enforce the policy WG_CIP_LH_SV.			
SOW Annex-A	[SRS-6-209]	WG_CIS_SV SHALL enforce WG_CIP_LH_SV based on the contents of the HTTP Message body.			
SOW Annex-A	[SRS-6-21]	The operation 'ForwardInternalNetworkLH' MUST support error handling as specified in [IETF RFC 7414, 2015].			
SOW Annex-A	[SRS-6-210]	WG_CIS_SV SHALL be able to check the body of an HTTP message for XML well-formedness.			
SOW Annex-A	[SRS-6-211]	WG_CIS_SV SHALL be able to validate the body of an HTTP message against a list LIST_WG_CIS_SV-XS of W3C XML Schemas (defined in the policy WG_CIP_LH_SV).			
SOW Annex-A	[SRS-6-212]	WG_CIS_SV SHALL be able to check that the namespace of the root node in the HTTP message body belongs to a list of namespaces LIST_WG_CIS_SV-NS (defined in the policy WG_CIP_LH_SV).			
SOW Annex-A	[SRS-6-213]	WG_CIS SHALL provide an HTTP header vetting capability WG_CIS_HV that comprises the filters that are executed in order to enforce the policies WG_CIP_HL_HV and WG_CIP_LH_HV.			
SOW Annex-A	[SRS-6-214]	WG_CIS_HV SHALL enforce WG_CIP_LH_HV and WG_CIP_HL_HV based on the following types of information attributes in the HTTP message header: • Start-line: o Method; o Request-URI; o HTTP-version; o Status-code. • Message-header: o Field-name; o Field-value.			
SOW Annex-A	[SRS-6-215]	WG_CIS_HV SHALL be able to verify the information attributes in [SRS-6-214] against the rulesets RULESET_WG_CIS_HV-HL and RULESET_WG_CIS_HV-LH (specified in the policies WG_CIP_HL_HV and WG_CIP_LH_HV respectively).			
SOW Annex-A	[SRS-6-216]	WG_CIS_HV SHALL be able to add, remove or rewrite entire header lines of an HTTP message.			
SOW Annex-A	[SRS-6-217]	WG_CIS_HV SHALL be able to add, remove or rewrite values of the information attributes in [SRS-6-214].			
SOW Annex-A	[SRS-6-218]	WG_CIS_HV SHALL be able to normalize URIs in header lines of an HTTP message (i.e. remove all unneeded or escaped characters from a URI and ensure sure all characters that require escaping are escaped).			
SOW Annex-A	[SRS-6-219]	WG_CIS MUST provide a label validation capability WG_CIS_LV that comprises the content filters that are executed in order to enforce the policy WG_CIP_HL_LV.			
SOW Annex-A	[SRS-6-22]	WG_DEX MUST offer a HyperText Transport Protocol (HTTP) v1.1 and v2, [IETF RFC 7230, 2014], [IETF RFC 7540, 2014] interface 'SOA Platform Services HL' on top of 'Communications Access Services HL'.			
SOW Annex-A	[SRS-6-220]	WG_CIS_LV MUST support the NATO standard ADatP-4774 "Confidentiality Metadata Label Syntax" [STANAG 4774].			
SOW Annex-A	[SRS-6-221]	WG_CIS_LV MUST support the NATO standard and ADatP-4778 "Metadata Binding Mechanism" [STANAG 4778].			
SOW Annex-A	[SRS-6-222]	WG_CIS_LV MUST support the binding approaches 'encapsulating' and 'embedded' as defined in [STANAG 4778].			
SOW Annex-A	[SRS-6-223]	WG_CIS_LV MAY support the binding approach 'detached' as defined in [STANAG 4778].			
SOW Annex-A	[SRS-6-224]	WG_CIS_LV MUST support the binding profile "Simple Object Access Protocol (SOAP) Binding Profile" in [STANAG 4778 SRD.2].			
SOW Annex-A	[SRS-6-225]	WG_CIS_LV MUST support the binding profile "Representational State Transfer (REST) Profile" in [STANAG 4778 SRD.2].			
SOW Annex-A	[SRS-6-226]	WG_CIS_LV MUST support the binding profile "XML Signature Cryptographic Artefact Profile" in [STANAG 4778 SRD.2].			
SOW Annex-A	[SRS-6-227]	WG_CIS_LV MUST support the binding profile "Digital Signature Cryptographic Artefact Profile" in [STANAG 4778 SRD.2].			
SOW Annex-A	[SRS-6-228]	WG_CIS_LV MUST support the binding profile "Keyed-Hash Message Authentication Code Cryptographic Artefact Profile" in [STANAG 4778 SRD.2].			
SOW Annex-A	[SRS-6-229]	WG_CIS_LV SHALL be able to validate a digital signature by invoking the operation 'Verify' (6.6.2.2.3) at the interface 'Public Key Cryptographic Services' ([SRS-6-239]) provided by WG_PKCS (6.6.2.1).			
SOW Annex-A	[SRS-6-23]	The interface 'SOA Platform Services HL' and its operations SHALL be conformant to the following service interface profiles (SIPs), see Appendix B.3: • Service Interface Profile for Security Services; • Service Interface Profile for REST Security Services; • Service Interface Profile for Messaging (SOAP); • Service Interface Profile for REST Messaging.			
SOW Annex-A	[SRS-6-230]	WG_CIS_LV SHALL be able to perform the validation of XML against a list LIST_WG_CIS_LV-XS of W3C XML Schemas (defined in the policy WG_CIP_HL_LV).			

SOW Annex-A	[SRS-6-231]	For a given child element *CE* , CIS_LV SHALL be able to match the value of *CE* and the values of attributes of *CE* against a list of values.			
SOW Annex-A	[SRS-6-232]	For a given HTTP message, WG_CIS_LV SHALL be able to evaluate the bindings in the HTTP message body *HB* and identify the set of data objects *S* in *HB* (or referenced in *HB*) that are labelled (i.e. for each data object *DO* in *S* there is a confidentiality metadata label *CL* that is bound to *DO*).			
SOW Annex-A	[SRS-6-233]	For a confidentiality metadata label *CL* that is bound to a data object *DO* , WG_CIS_LV SHALL be able to associate the following information attributes in *CL* (see [STANAG 4774]) with *DO* : • Policy identifier; • Classification; • Categories.			
SOW Annex-A	[SRS-6-234]	WG_CIS_LV SHALL be able to verify the values of the information attributes in ([SRS-6-233]) against a metadata policy information file MPIF_NATO.			
SOW Annex-A	[SRS-6-235]	WG_CIS_LV SHALL enforce the ruleset RULESET_WG_CIS_LV (specified in the policy WG_CIP_HL_LV) based on the information attributes in ([SRS-6-233]).			
SOW Annex-A	[SRS-6-236]	WG_CIS_LV MAY support the sanitization of data based on RULESET_WG_CIS_LV.			
SOW Annex-A	[SRS-6-237]	WG_CIS_LV SHALL be able to apply XML canonicalization to a data object.			
SOW Annex-A	[SRS-6-238]	WG_CIS_LV SHALL be able to generate a digital signature by invoking the operation 'Sign' (6.6.2.2.2) at the interface 'Public Key Cryptographic Services' ([SRS-6-239]) provided by WG_PKCS (6.6.2.1).			
SOW Annex-A	[SRS-6-239]	WG MUST provide a capability WG_PKCS that enables the WG to perform cryptographic operations and key management.			
SOW Annex-A	[SRS-6-24]	The interface 'SOA Platform Services HL' MUST support an operation 'ReceiveWebContentHL' that provides HTTP connectivity on the high domain.			
SOW Annex-A	[SRS-6-240]	WG_PKCS SHALL conform to the INFOSEC Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanisms [NAC AC/322-D/0047-REV2 (INV), 2009].			
SOW Annex-A	[SRS-6-241]	The cryptographic mechanisms implemented by WG_PKCS SHALL be based on Technical Implementation Guidance on Cryptographic Mechanisms in Support of Cryptographic Services [NAC AC/322-D(2012)0022, 2013].			
SOW Annex-A	[SRS-6-242]	WG_PKCS MUST offer an interface 'Public Key Cryptographic Services' that supports the following cryptographic operations: • Sign (6.6.2.2.2); • Verify (6.6.2.2.3); • Encrypt (6.6.2.2.4); • Decrypt (6.6.2.2.5).			
SOW Annex-A	[SRS-6-243]	For every action taken, the operations 'Sign', 'Verify', 'Encrypt' and 'Decrypt' SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log both the action and the result of the action.			
SOW Annex-A	[SRS-6-244]	The operation 'Sign' MUST support: • The generation of cryptographic bindings according to 'Cryptographic Artefact Binding Profiles' [STANAG 4778 SRD.2]. • The generation of XML digital signatures based on XMLDSIG Core Generation [W3C XMLDSIG-CORE, 2008]; • The generation of key-hashed message authentication code (HMAC, [IETF RFC 2104, 1997]) conformant with Transport Layer Security (TLS, [IETF RFC 8446, 2018]); • The generation of cryptographic digest values in accordance with a specified cryptographic algorithm: the Secure Hash Algorithm (SHA) [NIST FIPS-180-3, 2008] and lengths of cryptographic digest values of 160 bits, 256 bits, or 384 bits that meet the following: o Requirements defined in the "CIS Security Technical And Implementation Directive On The NATO PKI Certificate Policy" [NAC AC/322-D(2004)0024-REV3-COR1, 2018] and [NAC AC/322-D(2007)0002-REV1, 2015] o The XML Signature Syntax and Processing standard (Second Edition) [W3C XMLDSIG-CORE, 2008].			
SOW Annex-A	[SRS-6-245]	The operation 'Verify': • MUST support the validation of XML digital signatures based on XMLDSIG Core Validation [W3C XMLDSIG-CORE, 2008]; • MUST support validation of XML digital signatures in accordance with a specified cryptographic algorithm: the Rivest Shamir Adleman (RSA) algorithm [RSA PKCS#1, 2002] and cryptographic key sizes of 2048 bits that meet the following: o Requirements defined in the CIS Security Technical And Implementation Directive On The NATO PKI Certificate Policy [NAC AC/322-D(2004)0024-REV3-COR1, 2018] and [NAC AC/322-D(2007)0002-REV1, 2015] o The XML Signature Syntax and Processing standard (Second Edition) [W3C XMLDsig-2nd-Ed, 2008]. • MUST support signatures of the types XMLDSIG 'enveloping' and 'enveloped'. • MAY support signatures of the type XMLDSIG 'detached'. • MUST support the validation and of cryptographic bindings according to 'Cryptographic Artefact Binding Profiles' [STANAG 4778 SRD.2].			
SOW Annex-A	[SRS-6-246]	The operation 'Encrypt' MUST support encryption of data conformant with Transport Layer Security (TLS, [IETF RFC 8446, 2018]).			
SOW Annex-A	[SRS-6-247]	The operation 'Decrypt' MUST support decryption of data conformant with Transport Layer Security (TLS, [IETF RFC 8446, 2018]).			
SOW Annex-A	[SRS-6-248]	The WG MUST provide a management capability WG_MGMT that supports local and remote management of the WG.			
SOW Annex-A	[SRS-6-249]	For local management, WG_MGMT MUST offer an interface WG_IF_LOCAL_MGMT consisting of a directly attached keyboard and display console.			
SOW Annex-A	[SRS-6-25]	The operation 'ReceiveWebContentHL' MUST support Transport Layer Security (TLS, [IETF RFC 8446, 2018]).			
SOW Annex-A	[SRS-6-250]	WG_IF_LOCAL_MGMT SHALL support the invocation of the operations at the interfaces 'CIS Security' ([SRS-6-270]), 'SMC Configuration Management' ([SRS-6-288]) and 'Cyber Defence' (6.7.6.2).			
SOW Annex-A	[SRS-6-251]	WG_MGMT MUST provide a capability WG_MGMT_AM that allows Audit Administrators to fulfil their role.			
SOW Annex-A	[SRS-6-252]	WG_MGMT_AM MUST be interoperable with NATO auditing and system management tools.			
SOW Annex-A	[SRS-6-253]	WG_MGMT_AM SHALL provide the capability to detect and create records of security-relevant events associated with users.			
SOW Annex-A	[SRS-6-254]	WG_MGMT_AM SHALL provide the capability to detect and create records of security-relevant events associated with end users requests for accessing information cross domain.			
SOW Annex-A	[SRS-6-255]	WG_MGMT_AM SHALL provide the capability to appropriately classify and protect audit information in accordance with NATO security policy.			
SOW Annex-A	[SRS-6-256]	WG_MGMT_AM SHALL provide mechanisms to protect audit logs from unauthorised access, modification and deletion.			
SOW Annex-A	[SRS-6-257]	WG_MGMT_AM SHALL provide the capability to selectively view audit information, and alert the Audit Administrator of identified potential security violations.			
SOW Annex-A	[SRS-6-258]	WG_MGMT_AM SHALL provide reliable time stamps and the capability for the Audit Administrator to set the time used for these time stamps.			
SOW Annex-A	[SRS-6-259]	WG_MGMT_AM SHALL support the generation of an audit log for each of the following general auditable events: • WG start-up and shutdown; • WG Users logon and logoff; • Creation, modification (i.e. changes to permissions) or deletion of user accounts; • Changes to security related system management functions; • Audit log access; • Invocation of privileged operations; • Modification to WG access rights; • Unauthorised attempts to access WG system files; • All modified objects are recorded with date, time, details of change and user.			
SOW Annex-A	[SRS-6-26]	The operation 'ReceiveWebContentHL' MUST support the invocation of the operations 'Verify' (6.6.2.2.3) and 'Decrypt' (6.6.2.2.5) at the interface 'Public Key Cryptographic Services' ([SRS-6-239]) provided by WG_PKCS (6.6.2.1).			
SOW Annex-A	[SRS-6-260]	WG_MGMT_AM SHALL support the generation of an audit log for each of the following Data Exchange Services auditable events: • Data Exchange Services start-up and shutdown; • Unauthorised attempts to request access to information cross domain; • Unauthorised attempts to modify Data Exchange Services configuration; • Failed Data Exchange Services operations.			
SOW Annex-A	[SRS-6-261]	WG_MGMT_AM SHALL support the generation of an audit log for each of the following Protection Services auditable events: • Protection Services start-up and shutdown; • Failed Protection Services operations; • Unauthorised attempts to modify Protection Services configuration; • Creation, modification and deletion of Public Key Cryptographic Services keying material; • Updates of Content Inspection Services content filters; • Failed certificate path validation and revocation.			
SOW Annex-A	[SRS-6-262]	WG_MGMT_AM SHALL support the generation of an audit log for each of the following Protection Policy Enforcement Services auditable events: • Protection Policy Enforcement Services start-up and shutdown; • Failed Protection Policy Enforcement Services operations; • Unauthorised attempts to create, modify or delete Information Flow Control policies; • Unauthorised attempts to create, modify or delete Content Inspection policies.			
SOW Annex-A	[SRS-6-263]	WG_MGMT_AM SHALL support the archiving of the audit log after a period of time as configured by the Audit Administrator.			
SOW Annex-A	[SRS-6-264]	WG_MGMT_AM SHALL by default archive the audit log daily.			
SOW Annex-A	[SRS-6-265]	WG_MGMT_AM SHALL automatically back up audit logs at configurable intervals.			
SOW Annex-A	[SRS-6-266]	WG_MGMT_AM SHALL provide the capability, including integrity checking, to verify that the audit log has been archived correctly.			
SOW Annex-A	[SRS-6-267]	WG_MGMT_AM SHALL provide the capability to alert the Audit Administrator when the audit log exceeds a configurable percentage of the configurable maximum permitted size.			
SOW Annex-A	[SRS-6-268]	WG_MGMT_AM SHALL by default set the configurable percentage to 90% of the configurable maximum permitted size.			
SOW Annex-A	[SRS-6-269]	WG_MGMT MUST provide a capability WG_MGMT_CS that allows for the management of CIS Security information specific to the WG.			

SOW Annex-A	[SRS-6-27]	After receiving an HTTP message, the operation 'ReceiveWebContentHL' SHALL pass the HTTP message to the interface 'IFCPE Services High to Low' ([SRS-6-71]) for further processing.			
SOW Annex-A	[SRS-6-270]	WG_MGMT_CS MUST support the retrieval of key material, certificates and CRLs from locations external to the WG.			
SOW Annex-A	[SRS-6-271]	WG_MGMT_CS MUST support one or more of the following protocols and associated CIS Security Messages for the retrieval of key material, certificates and CRLs: • Secure LDAP (LDAPS) [IETF RFC 4510 – 4519, 2006]; • HTTP(S) ([IETF RFC 7230, 2014], [IETF RFC 7540, 2015]. [IETF RFC 8446, 2018], [IETF RFC 2818, 2000]; • SOAP ([W3C SOAP 1.1, 2000] and [W3C SOAP 1.2, 2007]).			
SOW Annex-A	[SRS-6-272]	WG_MGMT_CS SHALL check the status or certificates against CRLs in accordance with the NPKI Certificate Policy [NAC AC/322-D(2004)0024-REV3-COR1, 2018].			
SOW Annex-A	[SRS-6-273]	WG_MGMT_CS MAY support remote checking of the status of certificates using the Online Certificate Status protocol (OCSP) [IETF RFC 6960, 2013].			
SOW Annex-A	[SRS-6-274]	WG_MGMT_CS MUST support automated execution of the following actions: • Updating of certificates; • Updating of CRLs;			
SOW Annex-A	[SRS-6-275]	WG_MGMT_CS MUST support scheduling of each operation in [SRS-6-274] such that: • The operation will be executed at a configurable date and time, with: o date expressed in years, month and day; o time expressed in hours and minutes. • When starting at a configurable date and time, the operation will be executed at a configurable regular time interval expressed in days, weeks or months.			
SOW Annex-A	[SRS-6-276]	WG_MGMT_CS SHALL pass outgoing CIS Security Messages to the interface 'Core Services Management' (6.4.5.1) for further processing.			
SOW Annex-A	[SRS-6-277]	WG_MGMT_CS MUST offer an interface 'CIS Security' that accepts an incoming 'CIS Security Message' for further processing.			
SOW Annex-A	[SRS-6-278]	The interface 'CIS Security' MUST support an operation 'Manage Protection Policies' that provides the capability to manage the lifecycle of the IFPs and CIPs in support of WG_IFCPE ([SRS-6-70]) and WG_CIPE (6.5.3.1) respectively.			
SOW Annex-A	[SRS-6-279]	The operation 'Manage Protection Policies' SHALL support the following actions: • Create policy; • Read policy; • Update policy; • Delete policy; • Activate policy; • De-activate policy; • Backup policy; • Restore policy.			
SOW Annex-A	[SRS-6-28]	The operation 'ReceiveWebContentHL' SHALL persist the HTTP TCP/IP connection from an HTTP client in the high domain until: • an HTTP Response is received at the interface 'SOA Platform Services LH' (6.4.3.2) and processed by the operation 'ForwardWebContentLH' (6.4.3.2.3); or • the HTTP TCP/IP connection is timed out by the HTTP client.			
SOW Annex-A	[SRS-6-280]	WG_MGMT_CS MUST support the automated execution of those operations in [SRS-6-279] that comprise a policy update.			
SOW Annex-A	[SRS-6-281]	WG_MGMT_CS MUST support the automated execution of the operation 'Backup policy' in [SRS-6-279].			
SOW Annex-A	[SRS-6-282]	WG_MGMT_CS MUST support scheduling of policy updates such that: • The policy update will be executed at a configurable date and time, with: o date expressed in years, month and day; o time expressed in hours and minutes. • When starting at a configurable date and time, the policy update will be executed at a configurable regular time interval expressed in days, weeks or months.			
SOW Annex-A	[SRS-6-283]	The interface 'CIS Security' MUST support an operation 'Review' that provides the capability to review audit logs.			
SOW Annex-A	[SRS-6-284]	The interface 'CIS Security' MUST support an operation 'Manage Public Key Material' that provides the capability to manage key material to support WG_PKCS (6.6.2.1).			
SOW Annex-A	[SRS-6-285]	The operation 'Manage Public Key Material' SHALL be compliant with CIS Security Technical and Implementation Guidance in Support of Public Key Infrastructure - Cryptographic Artefacts [NAC AC/322-D(2007)0002-REV1, 2015].			
SOW Annex-A	[SRS-6-286]	The operation 'Manage Public Key Material' MUST provide the capability to: • Import and store key material; • Install and de-install certificates; • Update certificates; • Import and update CRLs.			
SOW Annex-A	[SRS-6-287]	WG_MGMT MUST provide a management capability WG_MGMT_CM that enables the configuration and management of the WG.			
SOW Annex-A	[SRS-6-288]	WG_MGMT_CM MUST provide the capability to change, capture, duplicate, backup or restore the configuration of the WG.			
SOW Annex-A	[SRS-6-289]	WG_MGMT_CM MUST provide the capability to remotely prepare a WG configuration WG_CONFIG and deploy WG_CONFIG onto multiple instances of the WG.			
SOW Annex-A	[SRS-6-29]	In support of the use of HTTP persistent connections, the WG SHALL be able to correlate HTTP request and response messages that belong to the same HTTP connection initiated in the high domain.			
SOW Annex-A	[SRS-6-290]	WG_MGMT_CM MUST offer a graphical user interface for all configuration and installation options, including the updating of XML artefacts (6.7.5).			
SOW Annex-A	[SRS-6-291]	WG_MGMT_CM MUST support configuration of the WG based on a customizable (pre-loaded) configuration templates (e.g. XML schemas are pre-installed) in support of common information exchange scenarios.			
SOW Annex-A	[SRS-6-292]	WG_MGMT_CM MUST support the creation and installation (pre-loading) of the configuration templates as described in [SRS-6-291].			
SOW Annex-A	[SRS-6-293]	WG_MGMT_CM MUST support the retrieval of XML artefacts from locations external to the WG.			
SOW Annex-A	[SRS-6-294]	WG_MGMT_CM MUST support one or more of the following management protocols and associated SMC Messages for the retrieval of XML artefacts: • Secure LDAP (LDAPS) [IETF RFC 4510 – 4519, 2006]; • HTTP(S) ([IETF RFC 7230, 2014], [IETF RFC 7540, 2015] [IETF RFC 8446, 2008], [IETF RFC 2818, 2000]; • SOAP ([W3C SOAP 1.1, 2000] and [W3C SOAP 1.2, 2007]).			
SOW Annex-A	[SRS-6-295]	WG_MGMT_CM MUST support automated execution of the following action: • Updating of XML artefacts including XML Schemas and MPIFs.			
SOW Annex-A	[SRS-6-296]	WG_MGMT_CM MUST support scheduling of the operation in [SRS-6-291] such that: • The operation will be executed at a configurable date and time, with: o date expressed in years, month and day; o time expressed in hours and minutes. • When starting at a configurable date and time, the operation will be executed at a configurable regular time interval expressed in days, weeks or months.			
SOW Annex-A	[SRS-6-297]	To track WG configuration information, WG_MGMT_CM SHALL interface to the enterprise configuration management database (BMC ITSM Atrium CMDB) via the interface 'SMC Configuration Management' in order to support the enterprise configuration management.			
SOW Annex-A	[SRS-6-298]	WG_MGMT_CM SHALL pass outgoing SMC Messages to the interface 'Core Services Management' (6.4.5.1) for further processing.			
SOW Annex-A	[SRS-6-299]	WG_MGMT_CM MUST offer an interface 'SMC Configuration Management' that accepts an incoming 'SMC Message' for further processing.			
SOW Annex-A	[SRS-6-3]	WG_IF_NET_HIGH MUST support an operation 'ReceiveHigh' that receives (transfer-in) data from the high domain for processing by the WG.			
SOW Annex-A	[SRS-6-30]	The operation 'ReceiveWebContentHL' MUST support error handling as specified in [IETF RFC 7231, 2014].			
SOW Annex-A	[SRS-6-300]	The interface 'SMC Configuration Management' MUST support an operation 'Configure OS' that provides the ability to configure and manage the operating system(s) and platform(s) the WG is running on, and the applications running on the operating system.			
SOW Annex-A	[SRS-6-301]	The operation 'Configure OS' SHALL support SMC Messages of the following types: • Secure Shell (SSH, [IETF RFC 4253, 2006]); • Network Time Protocol (NTP, [IETF RFC 5905, 2010]); • Intelligent Platform Management Interface (IPMI, [IPMI V2.0, 2013]); • Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]).			
SOW Annex-A	[SRS-6-302]	The interface 'SMC Configuration Management' MUST support an operation 'Configure Protection Policy Enforcement Services' that provides the capability to configure and manage WG_IFCPE ([SRS-6-70]) and WG_CIPE (6.5.3.1).			
SOW Annex-A	[SRS-6-303]	The operation 'Configure Protection Policy Enforcement Services' MUST provide the capability to change, capture, duplicate, backup or restore the configuration of WG_IFCPE and WG_CIPE.			
SOW Annex-A	[SRS-6-304]	The operation 'Configure Protection Policy Enforcement Services' SHALL support one or more SMC Messages of the following types: • Secure Shell (SSH, [IETF RFC 4253, 2006]); • Remote Desktop Protocol (RDP); • Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]).			
SOW Annex-A	[SRS-6-305]	The interface 'SMC Configuration Management' MUST support an operation 'Configure Data Exchange Services' that provides the capability to configure and manage WG_DEX ([SRS-6-1]).			
SOW Annex-A	[SRS-6-306]	The operation 'Configure Data Exchange Services' MUST provide the capability to change, capture, duplicate, backup or restore the configuration of WG_DEX.			

SOW Annex-A	[SRS-6-307]	The operation 'Configure Data Exchange Services' SHALL support SMC Messages of the following types: • Secure Shell (SSH, [IETF RFC 4253, 2006]); • Remote Desktop Protocol (RDP); • Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]).			
SOW Annex-A	[SRS-6-308]	The interface 'SMC Configuration Management' MUST support an operation 'Configure Protection Services' that provides the capability to configure and manage WG_CIS ([SRS-6-190]) and WG_PKCS (6.6.2.1).			
SOW Annex-A	[SRS-6-309]	The operation 'Configure Protection Services' MUST provide the capability to change, capture, duplicate, backup or restore the configuration of WG_CIS and WG_PKCS.			
SOW Annex-A	[SRS-6-31]	The interface 'SOA Platform Services HL' MUST support an operation 'ForwardWebContentHL' that provides HTTP connectivity on the low domain.			
SOW Annex-A	[SRS-6-310]	The operation 'Configure Protection Services' SHALL support SMC Messages of the following types: • Secure Shell (SSH, [IETF RFC 4253, 2006]); • Remote Desktop Protocol (RDP); • Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]).			
SOW Annex-A	[SRS-6-311]	The operation 'Configure Protection Services' MUST provide the capability to manage filters for WG_CIS.			
SOW Annex-A	[SRS-6-312]	The management of filters for WG_CIS SHALL include: • Installation and de-installation of content filters; • Updating of content filters.			
SOW Annex-A	[SRS-6-313]	The operation 'Configure Protection Services' MUST provide the capability to manage XML artefacts for WG_CIS.			
SOW Annex-A	[SRS-6-314]	The management of XML artefacts for WG_CIS SHALL include: • Loading and removal of XML artefacts (including XML Schemas and MPIFs); • Updating of XML artefacts.			
SOW Annex-A	[SRS-6-315]	WG_MGMT MUST provide a management capability WG_MGMT_CD that provides the capability to manage and respond to cyber-related attacks on the WG.			
SOW Annex-A	[SRS-6-316]	WG_MGMT_CD SHALL pass outgoing Cyber Defence Messages to interface 'Core Services Management' (6.4.5.1) for further processing.			
SOW Annex-A	[SRS-6-317]	WG_MGMT_CD MUST offer an interface 'Cyber Defence' that accepts an incoming 'Cyber Defence Message' for further processing.			
SOW Annex-A	[SRS-6-318]	The interface 'Cyber Defence' MUST support an operation 'Assess' that provides the capability to assess damage and attacks/faults of WG components that have been affected by attacks and faults.			
SOW Annex-A	[SRS-6-319]	The operation 'Assess' SHALL be able to support analysis and evaluation of an attack.			
SOW Annex-A	[SRS-6-32]	After receiving an HTTP Request message from the interface 'IFCPE Services High to Low', the operation 'ForwardWebContentHL' SHALL initiate a new HTTP connection - including the HTTP message - to an HTTP server on the low domain. The new HTTP connection SHALL not use the stateful HTTP protocol attributes associated with the connection in [SRS-6-28].			
SOW Annex-A	[SRS-6-320]	The operation 'Assess' SHALL be able to support the aggregation of cybersecurity-related log, alert, and event data to a central repository or log aggregator as provided by the monitoring infrastructure in use by NCSC.			
SOW Annex-A	[SRS-6-321]	The interface 'Cyber Defence' MUST support an operation 'Respond' that provides the capability to dynamically mitigate the risk identified by a suspected attack/fault.			
SOW Annex-A	[SRS-6-322]	The operation 'Respond' SHALL be able to support the controlling of traffic flows for the purpose of stopping or mitigating an attack or fault.			
SOW Annex-A	[SRS-6-323]	The controlling of traffic flow by WG_MGMT_CD SHALL include: • Termination; • Throttling to a certain level of bandwidth or with a certain delay; • Redirection.			
SOW Annex-A	[SRS-6-324]	The interface 'Cyber Defence' MUST support an operation 'Recover' that provides the capability to take the required action to recover from an attack/fault and restore the components of the WG that were affected by the attack/fault.			
SOW Annex-A	[SRS-6-325]	WG_MGMT MUST provide a management capability WG_MGMT_EM that enables the management of events.			
SOW Annex-A	[SRS-6-327]	WG_MGMT_EM SHALL collect events and support the forwarding of events to the event management system (EMS).			
SOW Annex-A	[SRS-6-328]	WG_MGMT_EM SHOULD support monitoring based on the Microsoft System Center Operations Manager (SCOM).			
SOW Annex-A	[SRS-6-329]	WG_MGMT_EM SHALL support SNMP v3 [IETF RFC 3412, 2002] with appropriate Management Information Bases (MIBs).			
SOW Annex-A	[SRS-6-33]	After receiving an HTTP Response message from the interface 'IFCPE Services High to Low', the operation 'ForwardWebContentHL' SHALL forward the HTTP message to the low domain using the persisted HTTP connection ([SRS-6-43]).			
SOW Annex-A	[SRS-6-330]	WG_MGMT_EM SHALL provide a toolset which allows WG Administrators to define, filter, correlate and group events according to their context, criticality, source and impacts.			
SOW Annex-A	[SRS-6-331]	WG_MGMT_EM SHALL provide an event correlation toolset that can be either customizable or adaptive to detect normal and abnormal behaviour patterns.			
SOW Annex-A	[SRS-6-332]	WG_MGMT_EM SHALL provide the capability to examine recorded historical logs and archives.			
SOW Annex-A	[SRS-6-333]	WG_MGMT_EM SHALL support the correlation of requests and responses in order to track all responses (or faults) with the correct request for information access.			
SOW Annex-A	[SRS-6-335]	WG_MGMT_EM SHALL provide an event management toolset which allows WG Administrators to customize the building and saving of reports.			
SOW Annex-A	[SRS-6-336]	The event management toolset SHALL support the provision of visibility on usage patterns over daily, monthly and variable periods.			
SOW Annex-A	[SRS-6-337]	The event management toolset SHALL support trend and abnormal behaviour analysis.			
SOW Annex-A	[SRS-6-338]	WG_MGMT_EM SHALL be able to generate reports of the following types: • Service Level Agreement (SLA) compliance reports; • Error/exception reports; • Service usage reports; • Other customizable reports based on captured metrics which can be filtered and sorted based on various criteria.			
SOW Annex-A	[SRS-6-339]	WG_MGMT_EM SHALL pass outgoing SMC Messages to interface 'Core Services Management' (6.4.5.1) for further processing.			
SOW Annex-A	[SRS-6-34]	The operation 'ForwardWebContentHL' MUST support Transport Layer Security (TLS, [IETF RFC 8446, 2018]).			
SOW Annex-A	[SRS-6-340]	WG_MGMT_EM MUST offer an interface 'Event Management' that generates and forwards 'SMC Messages' in support of the operations 'Log' (6.7.7.1.1), 'Alert' (6.7.7.1.2) and 'Report' (6.7.7.1.3).			
SOW Annex-A	[SRS-6-341]	The interface 'Event Management' MUST support an operation 'Log' that provides the capability to record events that occur in software, or messages between components.			
SOW Annex-A	[SRS-6-342]	The operation 'Log' SHALL support writing log messages to a log file.			
SOW Annex-A	[SRS-6-343]	The operation 'Log' MUST provide the capability to log request and response attributes. These include: • Time-stamp; • Source and target address(es); • URL; • Operation; • Size; • Unique request id (extracted from the request/response or automatically generated by WG_MGMT_EM).			
SOW Annex-A	[SRS-6-344]	The operation 'Log' MUST provide the capability to log attributes extracted from the HTTP headers and HTTP body.			
SOW Annex-A	[SRS-6-345]	The operation 'Log' MUST provide the capability to selectively log whole messages based on pre-configured criteria or filter (e.g. policy based).			
SOW Annex-A	[SRS-6-346]	The operation 'Log' SHALL support SMC Messages one or more of the following types: • Syslog [IETF RFC 5424, 2009]; • HTTP Message [IETF RFC 7230, 2014].			
SOW Annex-A	[SRS-6-347]	The interface 'Event Management' MUST support an operation 'Alert' that provides the capability to generate an alert event when the acceptable threshold for a service has been reached, or is approached within a certain range.			
SOW Annex-A	[SRS-6-348]	The operation 'Alert' SHALL be able to support the generation of an alert of type 'Warning' that indicates it is necessary to take action in order to prevent an exception occurring.			
SOW Annex-A	[SRS-6-349]	The operation 'Alert' SHALL be able to support the generation of an alert of type 'Exception' that indicates that a given service is operating below the normal predefined parameters/indicators.			
SOW Annex-A	[SRS-6-35]	The operation 'ForwardWebContentHL' MUST support the invocation of the operation 'Encrypt' (6.6.2.2.4) at the interface 'Public Key Cryptographic Services' ([SRS-6-239]) provided by WG_PKCS (6.6.2.1).			
SOW Annex-A	[SRS-6-350]	The operation 'Alert' SHALL support SMC Messages of the type SNMP v3 [IETF RFC, 3412, 2002].			
SOW Annex-A	[SRS-6-351]	The interface 'Event Management' MUST support an operation 'Report' that provides the capability to generate reports in support of compliance, auditing, billing and service value determination.			
SOW Annex-A	[SRS-6-352]	The operation 'Report' SHALL support SMC Messages of the type SNMP v3 [IETF RFC 3412, 2002].			
SOW Annex-A	[SRS-6-353]	WG_MGMT MUST provide a management capability WG_MGMT_PM that enables the management of the performance and capacity of the WG.			
SOW Annex-A	[SRS-6-354]	WG_MGMT_PM MUST SHALL provide customizable dashboards for monitoring selected statistics and metrics for WG services.			
SOW Annex-A	[SRS-6-355]	WG_MGMT_PM SHALL pass outgoing SMC Messages to interface 'Core Services Management' (6.4.5.1) for further processing.			
SOW Annex-A	[SRS-6-356]	WG_MGMT_PM MUST offer an interface 'Performance Management' that generates and forwards 'SMC Messages' in support of the operations 'Monitor'(6.7.8.2.2), 'Meter' (6.7.8.2.3) and 'Track Messages' (6.7.8.2.4).			
SOW Annex-A	[SRS-6-357]	The interface 'Performance Management' MUST support an operation 'Monitor' that provides the capability to observe and track the operations and activities of end users (services) on the WG.			
SOW Annex-A	[SRS-6-358]	The operation 'Monitor' SHALL support the real-time monitoring of WG services against expected Key Performance Indicators (KPI), SLA or other metric thresholds as configured.			
SOW Annex-A	[SRS-6-359]	The operation 'Monitor' SHALL support the monitoring service faults and exceptions.			
SOW Annex-A	[SRS-6-36]	The operation 'ForwardWebContentHL' MUST support error handling as specified in [IETF RFC 7231, 2014].			
SOW Annex-A	[SRS-6-360]	The operation 'Monitor' SHALL support SMC Messages of the type SNMP v3 [IETF RFC 3412, 2002].			

SOW Annex-A	[SRS-6-361]	The interface 'Performance Management' MUST support an operation 'Meter' that provides the capability to measure levels of resource utilization consumed by service subscribers.			
SOW Annex-A	[SRS-6-362]	The operation 'Meter' SHALL support the storing of measured data for the purpose of summarizing and analysis.			
SOW Annex-A	[SRS-6-363]	The operation 'Meter' SHALL provide the capability to collect and present the statistics on service utilisation broken down by end user or system.			
SOW Annex-A	[SRS-6-364]	The operation 'Meter' SHALL support the collection of statistics for a given end user or system or group of end user or system over specified periods of time.			
SOW Annex-A	[SRS-6-365]	The operation 'Meter' SHALL support SMC Messages of the type SNMP v3 [IETF RFC 3412, 2002].			
SOW Annex-A	[SRS-6-366]	The interface 'Performance Management' MUST support an operation 'Track Messages' that provides the capability to track, monitor and log all message routing and service invocation activities.			
SOW Annex-A	[SRS-6-367]	The operation 'Track Messages' SHALL provide the capability to track, monitor, and log all access requests for information from the high domain to the low domain.			
SOW Annex-A	[SRS-6-368]	The operation 'Track Messages' SHALL provide the capability to track, monitor, and log all responses to access requests for information from the high domain to the low domain.			
SOW Annex-A	[SRS-6-369]	The operation 'Track Messages' SHALL provide the capability to track, monitor, and log all access requests for information from the low domain to the high domain.			
SOW Annex-A	[SRS-6-37]	WG_DEX MUST offer a HyperText Transport Protocol (HTTP), v1.1 and v2, [IETF RFC 7230, 2014], [IETF RFC 7540, 2014] interface 'SOA Platform Services LH' on top of 'Communications Access Services LH'.			
SOW Annex-A	[SRS-6-370]	The operation 'Track Messages' SHALL provide the capability to track, monitor, and log all responses to access requests for information from the low domain to the high domain.			
SOW Annex-A	[SRS-6-371]	The operation 'Track Messages' SHALL support SMC Messages of the type SNMP v3 [IETF RFC 3412, 2002].			
SOW Annex-A	[SRS-6-372]	WG_PKCS SHALL support the use Simple Certificate Enrolment Protocol (SCEP) [IETF RFC 8894, 2020] to sign the impersonation certificates that are used to support the interception Transport Layer Security (TLS) version 1.2 protected web (HTTPS) traffic.			
SOW Annex-A	[SRS-6-373]	WG_PKCS SHOULD support the use of Enrolment over Secure Transport (EST) [IETF RFC 7030, 2013] to sign the impersonation certificates that are used to support the interception Transport Layer Security (TLS) version 1.2 protected web (HTTPS) traffic.			
SOW Annex-A	[SRS-6-374]	The PKE module SHALL be validated according to the Smart Card Protection Profile [SCSUG-SCPP, 2001] or validated to at least FIPS 140-2 Level 2 [NIST FIPS 1402, 2001], or otherwise verified to an equivalent level of functionality and assurance by a NATO nation COMSEC authority. Ref.: [NAC AC/322-D(2004)0024-REV3-COR1, 2018].			
SOW Annex-A	[SRS-6-375]	The PKE module used by the WG SHALL be a NATO-approved cryptographic module with NATO-approved methods for key management (i.e. generation, access, distribution, destruction, handling, and storage of keys), and for cryptographic operations (i.e. encryption, decryption, signature, hashing, key exchange, and random-number-generation services) as described in [NAC AC/322-D(2007)0002-REV1, 2015].			
SOW Annex-A	[SRS-6-376]	The PKE module SHALL be evaluated according to the US Government Basic Robustness PKE PP with CPV - Basic Package, CPV - Basic Policy Package, CPV - Policy Mapping Package, CPV - Name Constraints Package, PKI Signature Verification Package, Online Certificate Status Protocol Client Package and Audit Package at EAL 4.			
SOW Annex-A	[SRS-6-377]	Any operating system of the WG is a trusted and securely configured operating system. The operating system is evaluated according to [OSPP, 2010] extended with [OSPP EP-IV, 2010] and [OSPP EP-TB, 2010] (or equivalent) and configured according to relevant NATO guidance and directives. Ref.: [AC AC/322-D/0048-REV3, 2019]			
SOW Annex-A	[SRS-6-378]	If the WG is a distributed system *S* (consisting of one or more hardware platforms or operating systems) it SHALL implement measures that prevent eavesdropping on communication channels between the systems (hardware platforms or operating systems) that comprise *S*.			
SOW Annex-A	[SRS-6-379]	The operating system depends on the underlying platform, which consists of hardware (processors, memory, and devices) and firmware. The underlying platform MUST provide functions that allow the operating system to: (i) Protect devices and areas of main memory from being directly accessed (without that access being mediated by the operating system) by untrusted subjects. (ii) Protect any other function of the underlying platform from being used by untrusted subjects in a way that would violate the security policy of the operating system. (iii) Ensure that any information contained in a protected resource is not released when the resource is reallocated; this includes ensuring that no residual information from a previously relayed message is transmitted. (iv) Enable enforcement of direction of information flow between the WG components 'WG security policy enforcement', 'high side http connectivity' and 'low side http connectivity' in Figure 20.			
SOW Annex-A	[SRS-6-38]	The interface 'SOA Platform Services LH' and its operations SHALL be conformant to the following service interface profiles (SIPs), see Appendix A.3: • Service Interface Profile for Security Services; • Service Interface Profile for REST Security Services; • Service Interface Profile for Messaging (SOAP); • Service Interface Profile for REST Messaging.			
SOW Annex-A	[SRS-6-380]	The WG hardware and firmware MUST be selected such that requirement [SRS-6-377] is met[6].			
SOW Annex-A	[SRS-6-381]	The WG SHALL provide well specified administrator roles in order to isolate administrative actions, and to make the administrative functions available locally and remotely.			
SOW Annex-A	[SRS-6-382]	The WG SHALL display an advisory warning regarding use of the WG.			
SOW Annex-A	[SRS-6-383]	The WG SHALL provide a mode from which recovery or initial start-up procedures can be performed.			
SOW Annex-A	[SRS-6-384]	The WG SHALL provide all the functions and facilities necessary to support the WG Administrators in their management of the security of the WG, and restrict these functions and facilities from unauthorized use.			
SOW Annex-A	[SRS-6-385]	The WG SHALL provide a means to ensure that WG Administrators are not communicating with some other entity pretending to be the WG when supplying identification and authentication data.			
SOW Annex-A	[SRS-6-386]	The WG SHALL provide the ability for a CIS Security Administrator to revoke the user's access through the TOE and TOE's ability to mediate data traffic: if the CIS Security Administrator revokes a user's access (e.g. by revoking an administrative role from a user) or modifies an information flow policy, the TOE SHALL immediately enforce the new CIS-Security-Administrator-defined policy.			
SOW Annex-A	[SRS-6-387]	The WG SHALL provide the capability to detect and create records of security-relevant events associated with users.			
SOW Annex-A	[SRS-6-388]	The WG SHALL provide the capability to protect audit information.			
SOW Annex-A	[SRS-6-389]	The WG SHALL provide the capability to selectively view audit information, and alert the Audit Administrator of identified potential security violations.			
SOW Annex-A	[SRS-6-39]	The interface 'SOA Platform Services LH' MUST support an operation 'ReceiveWebContentLH' that provides HTTP connectivity on the low domain.			
SOW Annex-A	[SRS-6-390]	The WG SHALL provide reliable time stamps and the capability for a WG Administrator to set the time used for these time stamps.			
SOW Annex-A	[SRS-6-391]	The WG SHALL provide a means to detect and reject the replay of authentication data as well as other data and security attributes used by the WG-SF.			
SOW Annex-A	[SRS-6-392]	The WG SHALL provide mechanisms that mitigate attempts to exhaust resources provided by the WG and thus protect availability of high side resources.			
SOW Annex-A	[SRS-6-393]	The WG SHALL provide mechanisms that control a user's logical access to the WG and to explicitly deny access to specific users when appropriate.			
SOW Annex-A	[SRS-6-394]	The WG-SF SHALL maintain a domain for its own execution that protects itself and its resources from external interference, tampering and unauthorized disclosure.			
SOW Annex-A	[SRS-6-4]	WG_IF_NET_HIGH MUST support an operation 'ForwardHigh' that forwards (transfer-out) data that has been processed by the WG to the high domain.			
SOW Annex-A	[SRS-6-40]	The operation 'ReceiveWebContentLH' MUST support Transport Layer Security (TLS, [IETF RFC 8446, 2018]).			
SOW Annex-A	[SRS-6-41]	The operation 'ReceiveWebContentLH' MUST support the invocation of the operations 'Verify' (6.6.2.2.3) and 'Decrypt' (6.6.2.2.5) at the interface 'Public Key Cryptographic Services' ([SRS-6-239]) provided by WG_PKCS (6.6.2.1).			
SOW Annex-A	[SRS-6-42]	After receiving an HTTP message, the operation 'ReceiveWebContentLH' SHALL pass the HTTP message to the interface 'IFCPE Services Low to High' (6.5.1.2.2) for further processing.			
SOW Annex-A	[SRS-6-43]	The operation 'ReceiveWebContentLH' SHALL persist the HTTP TCP/IP connection from an HTTP client in the high domain until: • an HTTP Response is received at the interface 'SOA Platform Services HL' ([SRS-6-22]) and processed by the operation 'ForwardWebContentHL' (6.4.3.1.3); or • the HTTP TCP/IP connection is timed out by the HTTP client.			
SOW Annex-A	[SRS-6-44]	In support of the use of HTTP persistent connections, the WG SHALL be able to correlate HTTP Request and Response messages that belong to the same HTTP connection initiated in the low domain.			
SOW Annex-A	[SRS-6-45]	The operation 'ReceiveWebContentLH' MUST support error handling as specified in [IETF RFC 7231, 2014].			
SOW Annex-A	[SRS-6-46]	The interface 'SOA Platform Services LH' MUST support an operation 'ForwardWebContentLH' that provides HTTP connectivity on the high domain.			
SOW Annex-A	[SRS-6-47]	After receiving an HTTP Request message from the interface 'IFCPE Services Low to High', the operation 'ForwardWebContentLH' SHALL initiate a new HTTP connection - including the HTTP message - to an HTTP server on the high domain. The new HTTP connection SHALL not use the stateful HTTP protocol attributes associated with the connection in [SRS-6-43].			
SOW Annex-A	[SRS-6-48]	After receiving an HTTP Response message from the interface 'IFCPE Services Low to High', the operation 'ForwardWebContentLH' SHALL forward the HTTP message to the high domain using the persisted HTTP connection ([SRS-6-43]).			
SOW Annex-A	[SRS-6-49]	The operation 'ForwardWebContentLH' MUST support Transport Layer Security (TLS, [IETF RFC 8446, 2018]).			
SOW Annex-A	[SRS-6-5]	WG_DEX MUST offer a physical network interface WG_IF_NET_LOW that provides Ethernet connectivity to the low domain.			
SOW Annex-A	[SRS-6-50]	The operation 'ForwardWebContentLH' MUST support the invocation of the operation 'Encrypt' (6.6.2.2.4) at the interface 'Public Key Cryptographic Services' ([SRS-6-239]) provided by WG_PKCS (6.6.2.1).			
SOW Annex-A	[SRS-6-500]	If WG_IFP_CA_HL_IN or WG_IFP_CA_HL_OUT do not permit information flow, the WG SHALL execute the actions specified in WG_IFP_CA_HL.			

SOW Annex-A	[SRS-6-501]	The policy WG_CIP_LH_MD SHALL specify the actions ACTIONS-LH_MD that need to be performed by WG_CIS_MD.			
SOW Annex-A	[SRS-6-502]	ACTIONS-LH_MD SHOULD include the following actions based on RULESET_WG_CIS_MD: • Identify; • Verify; • Transform; • Block; • Quarantine, as specified in the NATO CIPE functional specification in [NC3A TN-1486, 2012].			
SOW Annex-A	[SRS-6-503]	ACTIONS-LH_MD SHALL include the action to exclude an HTTP Message from policy enforcement by WG_CIS_MD based on RULESET_WG_CIS_MD.			
SOW Annex-A	[SRS-6-504]	WG_CIP_LH_MD SHALL specify RULESET_WG_CIS_MD.			
SOW Annex-A	[SRS-6-505]	RULESET_WG_CIS_MD SHALL be configurable.			
SOW Annex-A	[SRS-6-506]	RULESET_WG_CIS_MD SHALL specify: • A default scan rule that ensures all HTTP Messages are scanned for known malware; • Whitelist of values for the information attributes in [SRS-6-510] for which an HTTP Message can be excluded from malware scanning; • Whitelist of information flow characteristics for which HTTP Messages belonging to that information flow can be excluded from malware scanning. These characteristics SHALL include: o Source and destination IP-address of the information flow.			
SOW Annex-A	[SRS-6-507]	WG_CIS SHALL support the message syntax of HTTP messages as defined in Hypertext Transfer Protocol - HTTP/2 [IETF RFC 7540, 2014].			
SOW Annex-A	[SRS-6-508]	WG_CIS SHALL provide a malware detection capability WG_CIS_MD that comprises the content filters that are executed in order to enforce the policy WG_CIP_LH_MD.			
SOW Annex-A	[SRS-6-509]	WG_CIS_MD SHALL be able to identify known malware in the contents of an HTTP Message (headers and body) and enforce WG_CIP_LH_MD on the HTTP Message.			
SOW Annex-A	[SRS-6-51]	The operation 'ForwardWebContentLH' MUST support error handling as specified in [IETF RFC 7231, 2014].			
SOW Annex-A	[SRS-6-510]	WG_CIS_MD SHALL enforce WG_CIP_LH_MD based on the following types of information attributes in the HTTP message header: • Start-line: o Method; o Request-URI; o HTTP-version; o Status-code. • Message-header: o Field-name; o Field-value.			
SOW Annex-A	[SRS-6-511]	WG_CIS_MD SHALL be able to verify the information attributes in [SRS-6-510] against the rulesets RULESET_WG_CIS_MD.			
SOW Annex-A	[SRS-6-512]	WG_CIS_MD SHALL use a malware/virus scanner which is approved for use in the NATO Enterprise.			
SOW Annex-A	[SRS-6-513]	The management of WG_CIS_MD, including the process of updating malware signatures, SHALL integrate with the NCI Agency management solution of existing malware detection solutions in the NATO Enterprise.			
SOW Annex-A	[SRS-6-514]	WG_CIS_MD SHALL support the migration of the configuration of existing malware detection solutions in the NATO Enterprise, to the WG.			
SOW Annex-A	[SRS-6-515]	The operation 'Assess' SHALL be able to support the collection of cybersecurity-related log, alert, and event data in accordance with the NATO Enterprise Security Monitoring Guidance [NCI Agency TR/2017/NCB010400/12, 2017] and the Technical and Implementation Directive on CIS Security [NAC AC/322-D/0048-REV3, 2019].			
SOW Annex-A	[SRS-6-516]	The operation 'Assess' SHALL be able to support the ingestion of cybersecurity-related log, alert, and event data in the SIEM solution that is operated by NCSC.			
SOW Annex-A	[SRS-6-517]	The operation 'Assess' SHALL ensure that all cyber-related log, alert, and event data can be parsed correctly by the SIEM solution that is operated by NCSC.			
SOW Annex-A	[SRS-6-52]	WG_DEX MUST offer UDP [IETF RFC 768, 1980] and IPv4 and IPv6, [IETF RFC 791, 1981], [IETF RFC 8200, 2017] over Ethernet interface 'Communications Access Services Management' on top of WG_IF_MGMT.			
SOW Annex-A	[SRS-6-53]	The interface 'Communications Access Services Management' MUST support an operation 'ReceiveNetworkManagement' that provides TCP/IP connectivity on the management domain by receiving IP traffic for processing by the WG.			
SOW Annex-A	[SRS-6-54]	The operation 'ReceiveNetworkManagement' MUST support error handling as specified in [IETF RFC 7414, 2015].			
SOW Annex-A	[SRS-6-55]	The interface 'Communications Access Services Management' MUST support an operation 'ForwardNetworkManagement' that forwards IP traffic to the management domain.			
SOW Annex-A	[SRS-6-56]	The operation 'ForwardNetworkManagement' MUST support error handling as specified in [IETF RFC 7414, 2015].			
SOW Annex-A	[SRS-6-57]	WG_DEX MUST offer an interface 'Core Services Management' on top of 'Communications Access Services Management'.			
SOW Annex-A	[SRS-6-58]	The interface 'Core Services Management' MUST support the following management protocols: • Transport Layer protocol [IETF RFC 4251, 2006]; • Simple Network Management Protocol (SNMP) Version 3 [IETF RFC 3410 – 3418, 2002]; • Syslog; • Network Time Protocol;			
SOW Annex-A	[SRS-6-59]	The interface 'Core Services Management' MAY support the following management protocol: • Intelligent Platform Management Interface (IPMI) [IPMI V2.0, 2013]; • Hyper-Text Transport Protocol (HTTP) v1.1 Web interface [IETF RFC 7230, 2014] [IETF RFC 7231, 2014]; Hyper-Text Transport Protocol (HTTP) v2 Web interface, [IETF RFC 7540, 2014] • Remote Desktop (RDP). • Remote Procedure Call (RPC). • Keyboard, video and mouse (KVM) over Ethernet; • Command Line interface (CLI) via Secure Shell (SSH)			
SOW Annex-A	[SRS-6-6]	WG_IF_NET_LOW MUST support an operation 'ReceiveLow' that receives (transfer-in) data from the low domain for processing by the WG.			
SOW Annex-A	[SRS-6-60]	The interface 'Core Services Management' MUST support an operation 'ReceiveManagementContent' that receives external management traffic for further processing.			
SOW Annex-A	[SRS-6-61]	The operation 'ReceiveManagementContent' MUST support Transport Layer Security (TLS, [IETF RFC 8446, 2018]).			
SOW Annex-A	[SRS-6-62]	The operation 'ReceiveManagementContent' MUST support the Secure Shell Protocol (SSH) [IETF RFC 4251, 2006].			
SOW Annex-A	[SRS-6-63]	The operation 'ReceiveManagementContent' MUST support the invocation of the operations 'Verify' (6.6.2.2.3) and 'Decrypt' (6.6.2.2.5) at the interface 'Public Key Cryptographic Services' ([SRS-6-239]) provided by WG_PKCS (6.6.2.1).			
SOW Annex-A	[SRS-6-64]	The operation 'ReceiveManagementContent' SHALL pass management content in the form of a management message to the appropriate interface offered by WG_MGMT ([SRS-6-252]) for further processing.			
SOW Annex-A	[SRS-6-65]	The interface 'Core Services Management' MUST support an operation 'ForwardManagementContent' that accepts outgoing management messages for further processing.			
SOW Annex-A	[SRS-6-66]	After receiving a management message from one of the interfaces offered by WG_MGMT ([SRS-6-252]), the operation 'ForwardManagementContent' SHALL forward the management message, as payload of the appropriate management protocol, to the management domain.			
SOW Annex-A	[SRS-6-67]	The operation 'ForwardManagementContent' MUST support Transport Layer Security (TLS, [IETF RFC 8446, 2018]).			
SOW Annex-A	[SRS-6-68]	The operation 'ForwardManagementContent' MUST support the Secure Shell Protocol (SSH) [IETF RFC 4251, 2006].			
SOW Annex-A	[SRS-6-69]	The operation 'ForwardManagementContent' MUST support the invocation of the operation 'Encrypt' (6.6.2.2.4) at the interface 'Public Key Cryptographic Services' ([SRS-6-239]) provided by WG_PKCS (6.6.2.1).			
SOW Annex-A	[SRS-6-7]	WG_IF_NET_LOW MUST support an operation 'ForwardLow' that forwards (transfer-out) data that has been processed by the WG to the low domain.			
SOW Annex-A	[SRS-6-70]	The WG MUST provide an information flow control policy enforcement (IFCPE) capability WG_IFCPE that enables the WG to: • Mediate the flow of information between WG_IF_NET_HIGH and WG_IF_NET_LOW in accordance with the WG information flow policy WG_IFP; • Control incoming and outgoing management traffic at WG_IF_MGMT in accordance with the WG information flow policy WG_IFP.			
SOW Annex-A	[SRS-6-71]	The design of WG_IFCPE SHALL be such that the enforcement of policies WG_CIP_LH_LV and WG_CIP_HL_SV can be supported (see 6.2.4).			
SOW Annex-A	[SRS-6-72]	For the flow of information from WG_IF_NET_HIGH to WG_IF_NET_LOW, WG_IFCPE MUST offer an interface 'IFCPE Services High to Low' that accepts information for further processing.			
SOW Annex-A	[SRS-6-73]	The interface 'IFCPE Services High to Low' MUST support an operation 'Enforce HL Communications IFCPE' that enforces the policy WG_IFP_CA_HL.			
SOW Annex-A	[SRS-6-74]	The operation 'Enforce HL Communications IFCPE' SHALL enforce the policy WG_IFP_CA_HL_IN on the following information flow: • Source: Communications Access Services HL Interface -> ReceiveInternalNetworkHL; • Destination: SOA Platform Services HL Interface -> ReceiveWebContentHL; • Information: HTTP(S) traffic; • Operation: pass HTTP(S) traffic by ensuring the following conditions: o WG_IFP_CA_HL_IN permits information flow.			

SOW Annex-A	[SRS-6-75]	The operation 'Enforce HL Communications IFCPE' SHALL enforce the policy WG_IFP_CA_HL_OUT on the following information flow: • Source: SOA Platform HL Interface -> ForwardWebContentHL; • Destination: Communications Access Services HL Interface -> ForwardNetworkHL; • Information: HTTP(S) traffic; • Operation: pass HTTP(S) traffic by ensuring the following conditions: o WG_IFP_CA_HL_OUT permits information flow.			
SOW Annex-A	[SRS-6-76]	For every action taken, the operation 'Enforce HL Communications IFCPE' SHALL invoke the operation 'Log' 6.7.7.1.1) at the interface 'Event Management' (6.7.7.1) and log the action.			
SOW Annex-A	[SRS-6-77]	If WG_IFP_CA_HL does not permit the release of information due to a policy violation, the WG SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' (6.7.7.1) and log the outcome O_WG_IFCPE (6.6.2.4).			
SOW Annex-A	[SRS-6-78]	The WG SHALL ensure that no illicit information flows exist to circumvent the enforcement of WG_IFP_CA_HL			
SOW Annex-A	[SRS-6-79]	The interface 'IFCPE Services High to Low' MUST support an operation 'Enforce HL SOA Platform IFCPE' that enforces the policy WG_IFP_SOA_HL.			
SOW Annex-A	[SRS-6-8]	WG_DEX SHOULD offer a physical network interface WG_IF_MGMT that provides Ethernet connectivity to the management domain.			
SOW Annex-A	[SRS-6-80]	Prior to enforcing WG_IFP_SOA_HL, WG_IFCPE SHALL completely reassemble all chunks of an HTTP message-body that was received with chunked transfer encoding.			
SOW Annex-A	[SRS-6-81]	The operation 'Enforce HL SOA Platform IFCPE' SHALL enforce the policy WG_IFP_SOA_HL on the following information flow: • Source: SOA Platform Services HL Interface->ReceiveWebContentHL; • Destination: SOA Platform Services HL Interface >ForwardWebContentHL; • Information: HTTP Messages; • Operation: pass HTTP Messages from source to destination ensuring the following conditions: o the HTTP Message has been processed by the WG content inspection policy enforcement capability WG_CIPE (6.5.3.1) based on the content inspection policy WG_CIP_HL ([SRS-6-144]); o Based on the outcome of processing by WG_CIPE, WG_IFP_SOA_HL permits the release of the HTTP Message to the low domain. o In case of an HTTP response message, pass message only if it was preceded by an HTTP request message that was passed as part of the enforcement of WG_IFP_SOA_LH ([SRS-6-97]).			
SOW Annex-A	[SRS-6-82]	The operation 'Enforce HL SOA Platform IFCPE' MUST support the invocation of the operation 'Enforce HL SOA CIPE' at the interface 'CIPE Services High to Low' (6.5.3.2). The operation 'Enforce HL SOA CIPE' SHALL take as input: • The HTTP message that is being processed; • The policy WG_CIP_HL.			
SOW Annex-A	[SRS-6-83]	If WG_IFP_SOA_HL does not permit the release of information, the WG SHALL execute the actions specified in WG_IFP_SOA_HL.			
SOW Annex-A	[SRS-6-84]	For every action taken, the operation 'Enforce HL SOA Platform IFCPE' SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the action.			
SOW Annex-A	[SRS-6-85]	If WG_IFP_SOA_HL does not permit the release of information due to a policy violation, the WG SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the outcome O_WG_IFCPE ([SRS-6-115]).			
SOW Annex-A	[SRS-6-86]	The WG SHALL ensure that no illicit information flows exist to circumvent the enforcement of WG_IFP_SOA_HL.			
SOW Annex-A	[SRS-6-87]	For the flow of information from WG_IF_NET_LOW to WG_IF_NET_HIGH, WG_IFCPE MUST offer an interface 'IFCPE Services Low to High' that accepts information for further processing.			
SOW Annex-A	[SRS-6-88]	The interface 'IFCPE Services Low to High' MUST support an operation 'Enforce LH Communications IFCPE' that enforces the policy WG_IFP_CA_LH.			
SOW Annex-A	[SRS-6-89]	The operation 'Enforce LH Communications IFCPE' SHOULD enforce the policy WG_IFP_CA_LH_IN on the following information flow: • Source: Communications Access Services LH Interface -> ReceiveInternalNetworkLH; • Destination: SOA Platform Services LH Interface -> ReceiveWebContentLH; • Information: HTTP(S) traffic; • Operation: pass HTTP(S) traffic by ensuring the following conditions: o WG_IFP_CA_LH_IN permits information flow.			
SOW Annex-A	[SRS-6-9]	If WG_DEX does not offer a physical network interface WG_IF_MGMT, it MUST offer a logical network interface WG_IF_MGMT on top of WG_IF_NET_HIGH.			
SOW Annex-A	[SRS-6-90]	The operation 'Enforce LH Communications IFCPE' SHOULD enforce the policy WG_IFP_CA_LH_OUT on the following information flow: • Source: SOA Platform LH Interface -> ForwardWebContentLH; • Destination: Communications Access Services LH Interface -> ForwardNetworkLH; • Information: HTTP(S) traffic; • Operation: pass HTTP(S) traffic by ensuring the following conditions: o WG_IFP_CA_LH_OUT permits information flow.			
SOW Annex-A	[SRS-6-91]	If WG_IFP_CA_LH_IN or WG_IFP_CA_LH_OUT do not permit information flow, the WG SHALL execute the actions specified in WG_IFP_CA_LH.			
SOW Annex-A	[SRS-6-92]	For every action taken, the operation 'Enforce LH Communications IFCPE' SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the action.			
SOW Annex-A	[SRS-6-93]	If WG_IFP_CA_LH does not permit the release of information due to a policy violation, the WG SHALL invoke the operation 'Log' (6.7.7.1.1) at the interface 'Event Management' ([SRS-6-342]) and log the outcome O_WG_IFCPE ([SRS-6-115]).			
SOW Annex-A	[SRS-6-94]	The WG SHALL ensure that no illicit information flows exist to circumvent the enforcement of WG_IFP_CA_LH.			
SOW Annex-A	[SRS-6-95]	The interface 'IFCPE Services Low to High' MUST support an operation 'Enforce LH SOA Platform IFCPE' that enforces the policy WG_IFP_SOA_LH.			
SOW Annex-A	[SRS-6-96]	Prior to enforcing WG_IFP_SOA_LH, WG_IFCPE SHALL completely reassemble all chunks of an HTTP message-body that was received with chunked transfer encoding.			
SOW Annex-A	[SRS-6-97]	The operation 'Enforce LH SOA Platform IFCPE' SHALL enforce the policy WG_IFP_SOA_LH on the following information flow: • Source: SOA Platform Services LH Interface->ReceiveWebContentLH; • Destination: SOA Platform Services LH Interface >ForwardWebContentLH; • Information: HTTP Messages; • Operation: pass HTTP Messages from source to destination ensuring the following conditions: o the HTTP Message has been processed by the WG content inspection policy enforcement capability WG_CIPE (6.5.3.1) based on the content inspection policy WG_CIP_LH ([SRS-6-151]). o Based on the outcome of processing by WG_CIPE, WG_IFP_SOA_LH permits the import of the HTTP Message to the high domain. o In case of an HTTP response message, pass message only if it was preceded by an HTTP request message that was passed as part of the enforcement of WG_IFP_SOA_HL ([SRS-6-81]).			
SOW Annex-A	[SRS-6-98]	The operation 'Enforce LH SOA Platform IFCPE' MUST support the invocation of the operation 'Enforce LH SOA CIPE' at the interface 'CIPE Services Low to High' (6.5.3.2). The operation 'Enforce LH SOA CIPE' SHALL take as input: • The HTTP message that is being processed; • The policy WG_CIP_LH.			
SOW Annex-A	[SRS-6-99]	If WG_IFP_SOA_LH does not permit the release of information, the WG SHALL execute the actions specified in WG_IFP_SOA_LH.			
SOW Annex-A	[SRS-7-1]	The MG MUST provide a data exchange capability MG_DEX that facilitates the mediation of data between the high domain and the low domain.			
SOW Annex-A	[SRS-7-10]	MG_IF_MGMT SHALL support an operation 'ReceiveManagement' that receives data from the management domain for processing by the MG.			
SOW Annex-A	[SRS-7-100]	For the flow of information from MG_IF_NET_LOW to MG_IF_NET_HIGH, MG_IFCPE MUST offer an interface 'IFCPE Services Low to High' that accepts information for further processing.			
SOW Annex-A	[SRS-7-101]	The interface 'IFCPE Services Low to High' MUST support an operation 'Enforce LH Communications IFCPE' that enforces the policy MG_IFP_CA_LH.			
SOW Annex-A	[SRS-7-102]	The operation 'Enforce LH Communications IFCPE' SHOULD enforce the policy MG_IFP_CA_LH_IN on the following information flow: • Source: Communications Access Services LH Interface -> ReceiveInternalNetworkLH; • Destination: Business Support Services LH Interface -> ReceiveEmailLH; • Information: SMTP(S) traffic; • Operation: pass SMTP(S) traffic by ensuring the following conditions: o MG_IFP_CA_LH_IN permits information flow.			
SOW Annex-A	[SRS-7-103]	The operation 'Enforce LH Communications IFCPE' SHOULD enforce the policy MG_IFP_CA_LH_OUT on the following information flow: • Source: Business Support Services LH Interface -> ForwardEmailLH; • Destination: Communications Access Services LH Interface -> ForwardEmailLH; Information: SMTP(S) traffic; • Operation: pass SMTP(S) traffic by ensuring the following conditions: o MG_IFP_CA_LH_OUT permits information flow.			
SOW Annex-A	[SRS-7-104]	For every action taken, the operation 'Enforce LH Communications IFCPE' SHALL invoke the operation 'Log' (7.7.7.1.1) at the interface 'Event Management' ([SRS-7-392]) and log the action.			
SOW Annex-A	[SRS-7-105]	If MG_IFP_CA_LH does not permit the release of information due to a policy violation, the MG SHALL invoke the operation 'Log' (7.7.7.1.1) at the interface 'Event Management' ([SRS-7-392]) and log the outcome O_MG_IFCPE ([SRS-7-91]).			
SOW Annex-A	[SRS-7-106]	The MG SHALL ensure that no illicit information flows exist to circumvent the enforcement of MG_IFP_CA_LH.			

SOW Annex-A	[SRS-7-107]	The Business Support Services IFCPE SHALL enforce the information flow control policy to mediate the flow of email between the Low Domain and the High Domain.			
SOW Annex-A	[SRS-7-108]	The Business Support Services IFCPE SHALL maintain a separate Business Support Services IFCP for the flow of information from the Low Domain to the High Domain (IEG-C_IFP_BS_EMAIL_LH).			
SOW Annex-A	[SRS-7-109]	The Business Support Services IFCP from the Low Domain to the High Domain (IEG-C_IFP_BS_EMAIL_LH) shall identify a Business Support Service CIP (IEG-C_CIP_BS_EMAIL_LH) (see section 7.2.3).			
SOW Annex-A	[SRS-7-11]	MG_IF_MGMT SHALL support an operation 'ForwardManagement' that forwards data that has been processed by the MG to the management domain.			
SOW Annex-A	[SRS-7-110]	The Enforce LH Business Support IFCPE operation SHALL call the Enforce LH Business Support CIP operation to determine if the email message from the Low Domain is compliant with the CIP (see section 7.2.3).			
SOW Annex-A	[SRS-7-111]	For incoming and outgoing management traffic at MG_IF_MGMT, MG_IFCPE MUST offer an interface 'IFCPE Services Management' that accepts information for further processing.			
SOW Annex-A	[SRS-7-112]	The interface 'IFCPE Services Management' MUST support an operation 'Enforce Management Communications IFCPE' that enforces the policy MG_IFP_MGMT.			
SOW Annex-A	[SRS-7-113]	The operation 'Enforce Management Communications IFCPE' SHALL enforce the policy MG_IFP_MGMT_IN on the following information flow: • Source: Communications Access Services Management Interface -> ReceiveNetworkManagement • Destination: Core Services Management Interface -> ReceiveManagementContent • Information: Management traffic. • Operation: pass management traffic by ensuring the following conditions: o Management traffic is filtered based on source IP addresses and ports, destination IP addresses, ports and protocol fields; o MG_IFP_MGMT_IN permits information flow.			
SOW Annex-A	[SRS-7-114]	The operation 'Enforce Management Communications IFCPE' SHALL enforce the policy MG_IFP_MGMT_OUT on the following information flow: • Source: Core Services Management Interface -> ForwardManagementContent • Destination: Communications Access Services Management Interface -> ForwardNetworkManagement • Information: Management traffic. • Operation: pass management traffic by ensuring the following conditions: o Management traffic is filtered based on source IP addresses and ports, destination IP addresses, ports and protocol fields; o MG_IFP_MGMT_OUT permits information flow.			
SOW Annex-A	[SRS-7-115]	If MG_IFP_MGMT_IN or MG_IFP_MGMT_OUT do not permit information flow, the MG SHALL execute the action specified in MG_IFP_MGMT.			
SOW Annex-A	[SRS-7-116]	For every action taken, the operation 'Enforce Management Communications IFCPE' SHALL invoke the operation 'Log' (7.7.1.1) at the interface 'Event Management' ([SRS-7-392]) and log the action.			
SOW Annex-A	[SRS-7-117]	If MG_IFP_MGMT does not permit the release of information due to a policy violation, the MG SHALL invoke the operation 'Log' 7.7.7.1.1) at the interface 'Event Management' ([SRS-7-392]) and log the outcome O_MG_IFCPE ([SRS-7-91]).			
SOW Annex-A	[SRS-7-118]	The MG SHALL ensure that no illicit information flows exist to circumvent the enforcement of MG_IFP_MGMT.			
SOW Annex-A	[SRS-7-119]	MG_IFP SHALL be configurable.			
SOW Annex-A	[SRS-7-12]	MG_DEX MUST offer a IPv4 and IPv6, [IETF RFC 791, 1981], and [IETF RFC 8200, 2017] over Ethernet interface 'Communications Access Services HL' on top of MG_IF_NET_HIGH and MG_IF_NET_LOW.			
SOW Annex-A	[SRS-7-120]	MG_IFP SHALL specify the actions ACTIONS that need to be executed by MG_IFCPE.			
SOW Annex-A	[SRS-7-121]	For each action in ACTIONS it SHALL be possible to: • Enable or disable the action. • Instruct MG_IFCPE to ignore the outcome of the execution of the action. • If the outcome O_MG_IFCPE of the execution of the action is negative (e.g. verification or validation fails, or a policy violation was determined): instruct MG_IFCPE to continue the enforcement of MG_IFP, or to stop.			
SOW Annex-A	[SRS-7-122]	It SHALL be possible to enable or disable the enforcement of each of the following sub-policies: • MG_IFP_CA_LH_IN; • MG_IFP_CA_LH_OUT; • MG_IFP_CA_HL_IN; • MG_IFP_CA_HL_OUT; • MG_IFP_MGMT_IN; • MG_IFP_MGMT_OUT; • MG_IFP_BS_LH; • MG_IFP_BS_HL.			
SOW Annex-A	[SRS-7-123]	MG_IFP SHALL specify the level of granularity of the outcome O_MG_IFCPE.			
SOW Annex-A	[SRS-7-124]	It SHALL be possible for MG_IFCPE to distinguish within O_MG_IFCPE: • The sub-policy ([SRS-7-122]) that was enforced when a policy violation was determined; • Identification of the action that led to the policy violation; • Reason for policy violation.			
SOW Annex-A	[SRS-7-125]	The policies MG_IFP_CA_HL, MG_IFP_CA_LH and MG_IFP_MGMT SHALL specify: • That an information flow (as described in 7.5.1.2.2, 7.5.1.3.2 and 7.5.1.4.1 respectively) is not permitted if the outcome O_MG_IFCPE constitutes a policy violation; • The action the MG shall take in case information flow is not permitted. The possible actions SHALL include: o Silently drop traffic; o Reset the TCP/IP connection.			
SOW Annex-A	[SRS-7-126]	The policy MG_IFP_CA_HL_IN SHALL specify the actions ACTIONS_MG_CA_HL_IN that the operation 'Enforce HL Communications IFCPE' SHALL execute for the information flow described in ([SRS-7-86]).			
SOW Annex-A	[SRS-7-127]	ACTIONS_MG_CA_HL_IN SHALL include the following actions: • Filter traffic based on the ruleset RULESET_MG_IFCPE-CA_HL_IN.			
SOW Annex-A	[SRS-7-128]	The policy MG_IFP_CA_LH_IN SHALL specify the actions ACTIONS_MG_CA_LH_IN that the operation 'Enforce LH Communications IFCPE' SHALL execute for the information flow described in 7.5.1.2.4.2.			
SOW Annex-A	[SRS-7-129]	ACTIONS_MG_CA_LH_IN SHALL include the following actions: • Filter traffic based on the ruleset RULESET_MG_IFCPE-CA_LH_IN.			
SOW Annex-A	[SRS-7-13]	The interface 'Communications Access Services HL' MUST support an operation 'ReceiveInternalNetworkHL' on top of MG_IF_NET_HIGH that provides TCP/IP connectivity on the high domain by receiving IP traffic for processing by the MG.			
SOW Annex-A	[SRS-7-130]	The policy MG_IFP_CA_LH_OUT SHALL specify the actions ACTIONS_MG_CA_LH_OUT that the operation 'Enforce LH Communications IFCPE' SHALL execute for the information flow described in ([SRS-7-103]).			
SOW Annex-A	[SRS-7-131]	ACTIONS_MG_CA_LH_OUT SHALL include the following actions: • Filter traffic based on the ruleset RULESET_MG_IFCPE-CA_LH_OUT.			
SOW Annex-A	[SRS-7-132]	The policy MG_IFP_MGMT_IN SHALL specify the actions ACTIONS_MG_MGMT_IN that the operation 'Enforce Management Communications IFCPE' SHALL execute for the information flow described in ([SRS-7-88]).			
SOW Annex-A	[SRS-7-133]	The policy MG_IFP_MGMT_OUT SHALL specify the actions ACTIONS_MG_MGMT_OUT that the operation 'Enforce Management Communications IFCPE' SHALL execute for the information flow described in ([SRS-7-102]).			
SOW Annex-A	[SRS-7-134]	ACTIONS_MG_MGMT_OUT SHALL include the following actions: • Filter traffic based on the ruleset RULESET_MG_IFCPE-MGT_OUT.			
SOW Annex-A	[SRS-7-135]	The policy MG_IFP_CA_HL SHALL specify RULESET_MG_IFCPE-CA_HL_IN and RULESET_MG_IFCPE-CA_HL_OUT.			
SOW Annex-A	[SRS-7-136]	RULESET_MG_IFCPE-CA_HL_IN and RULESET_MG_IFCPE-CA_HL_OUT SHALL be configurable.			
SOW Annex-A	[SRS-7-137]	The policy MG_IFP_CA_LH SHALL specify RULESET_MG_IFCPE-CA_LH_IN and RULESET_MG_IFCPE-CA_LH_OUT.			
SOW Annex-A	[SRS-7-138]	RULESET_MG_IFCPE-CA_LH_IN and RULESET_MG_IFCPE-CA_LH_OUT SHALL be configurable.			
SOW Annex-A	[SRS-7-139]	The policy MG_IFP_MGMT SHALL specify RULESET_MG_IFCPE-MGT_IN and RULESET_MG_IFCPE-MGT_OUT.			
SOW Annex-A	[SRS-7-14]	The operation 'ReceiveInternalNetworkHL' MUST support error handling as specified in [IETF RFC 7414, 2015].			
SOW Annex-A	[SRS-7-140]	RULESET_MG_IFCPE-MGT_IN and RULESET_MG_IFCPE-MGT_OUT SHALL be configurable.			
SOW Annex-A	[SRS-7-141]	Each of the rulesets RULESET_MG_IFCPE-CA_HL_IN, RULESET_MG_IFCPE-CA_HL_OUT, RULESET_MG_IFCPE-CA_LH_IN, RULESET_MG_IFCPE-CA_LH_OUT, RULESET_MG_IFCPE-MGT_IN, RULESET_MG_IFCPE-MGT_OUT SHALL include: • Identification of traffic flow that is allowed or disallowed based on source and destination IP addresses; • Identification of traffic that is allowed or disallowed based on protocols and ports; • Identification of traffic that is allowed or disallowed based on values of protocol fields.			
SOW Annex-A	[SRS-7-142]	The policy MG_IFP_BS_HL SHALL specify: • That a release of information to the low domain is not permitted if O_MG_CIPE_HL ([SRS-7-178]) constitutes a policy violation; • The action the MG shall take in case of a policy violation, see [SRS-7-144]			
SOW Annex-A	[SRS-7-143]	The policy MG_IFP_BS_LH SHALL specify: • That an import of information to the high domain is not permitted if O_MG_CIPE_LH ([SRS-7-184]) constitutes a policy violation; • The action the MG shall take in case of a policy violation, see [SRS-7-144].			
SOW Annex-A	[SRS-7-144]	The policies MG_IFP_BS_HL and MG_IFP_BS_LH SHALL specify a list of actions the MG shall take for non-compliant email messages.			
SOW Annex-A	[SRS-7-145]	The possible actions for non-compliant email messages SHALL include: • MG_IFP_ACTION_NONCOMPLIANT • MG_IFP_ACTION_NOTIFY • MG_IFP_ACTION_ALERT			
SOW Annex-A	[SRS-7-146]	The policies MG_IFP_BS_HL and MG_IFP_BS_LH SHALL specify the actions the MG shall take for compliant email messages.			

SOW Annex-A	[SRS-7-147]	The actions for compliant email messages SHALL include: • MG_IFP_ACTION_COMPLIANT • MG_IFP_ACTION _JOURNAL • MG_IFP_ACTION_ALERT			
SOW Annex-A	[SRS-7-148]	The Business Support Services IFCP SHALL support a configurable action (MG_IFP_ACTION_NONCOMPLIANT) which processes the non-compliant email message.			
SOW Annex-A	[SRS-7-149]	MG_IFP_ACTION_NONCOMPLIANT action SHALL support an option (DROP) to silently drop the email message from the information flow (i.e. the email message is not transferred to the recipients and a delivery status notification is not returned to the originator).			
SOW Annex-A	[SRS-7-15]	The interface 'Communications Access Services HL' MUST support an operation 'ForwardInternalNetworkHL' on top of MG_IF_NET_LOW that forwards IP traffic to the low domain.			
SOW Annex-A	[SRS-7-150]	MG_IFP_ACTION_NONCOMPLIANT action SHALL support an option (NON-DELIVER) to non-deliver the non-compliant email message (i.e. the message is not transferred to the recipients and a delivery status notification is returned to the originator).			
SOW Annex-A	[SRS-7-151]	MG_IFP_ACTION_NONCOMPLIANT action with the option NON-DELIVER SHALL generate a delivery status notification in accordance with [IETF RFC 3464, 2003].			
SOW Annex-A	[SRS-7-152]	MG_IFP_ACTION_NONCOMPLIANT action SHALL support an option (QUARANTINE) to hold the email message in quarantine (i.e. the message is not transferred to the recipients and a delivery status notification is not returned to the originator).			
SOW Annex-A	[SRS-7-153]	The email messages that are placed into quarantine SHALL be held in quarantine until either released (to the recipients) or deleted by an administrator.			
SOW Annex-A	[SRS-7-154]	The BSS_IFCP_ACTION_NONCOMPLIANT action SHALL only be configured with one of the options (DROP, NON-DELIVER or QUARANTINE).			
SOW Annex-A	[SRS-7-155]	The Business Support Services IFCP SHALL support a configurable action (MG_IFP_ACTION_JOURNAL) which processes a non-compliant email message.			
SOW Annex-A	[SRS-7-156]	The MG_ICP_ACTION_JOURNAL action SHALL be capable of being either enabled or disabled with an IFCP.			
SOW Annex-A	[SRS-7-157]	The MG_IFP_ACTION_JOURNAL action SHALL forward a copy of the non-compliant email message to a configurable email recipient.			
SOW Annex-A	[SRS-7-158]	The Business Support Services IFCP SHALL support a configurable action (MG_IFP_ACTION_NOTIFY) which processes a non-compliant email message.			
SOW Annex-A	[SRS-7-159]	MG_IFP_ACTION_NOTIFY action SHALL be capable of being either enabled or disabled with an IFCP.			
SOW Annex-A	[SRS-7-16]	The operation 'ForwardInternalNetworkHL' MUST support error handling as specified in [IETF RFC 7414, 2015].			
SOW Annex-A	[SRS-7-160]	MG_IFP_ACTION_NOTIFY action SHALL support an option (ORIGINATOR) to send the notification message to the originator of the non-compliant email message.			
SOW Annex-A	[SRS-7-161]	MG_IFP_ACTION_NOTIFY action SHALL support an option (RECIPIENTS) to send the notification message to the intended recipients of the non-compliant email message.			
SOW Annex-A	[SRS-7-162]	MG_IFP_ACTION_NOTIFY action SHALL support an option (ADMINISTRATOR) to send the notification message to a configurable administrator recipient.			
SOW Annex-A	[SRS-7-163]	MG_IFP_ACTION_NOTIFY action SHALL be configured with zero or more of the options (ORIGINATOR, RECIPIENTS and ADMINISTRATOR).			
SOW Annex-A	[SRS-7-164]	The Business Support Services IFCP SHALL support a configurable action (MG_IFP_ACTION_COMPLIANT) which processes the compliant email message.			
SOW Annex-A	[SRS-7-165]	MG_IFP_ACTION_COMPLIANT action SHALL always being enabled within an IFCP.			
SOW Annex-A	[SRS-7-166]	MG_IFP_ACTION_COMPLIANT action SHALL release the compliant message to the recipient domain.			
SOW Annex-A	[SRS-7-167]	The Business Support Services IFCP SHALL support a configurable action (MG_IFP_ACTION_JOURNAL) which processes the compliant email message.			
SOW Annex-A	[SRS-7-168]	The MG_IFP_ACTION_JOURNAL action SHALL forward a copy of the compliant email message to a configurable email recipient.			
SOW Annex-A	[SRS-7-169]	The MG SHALL provide a content inspection policy enforcement (CIPE) capability MG_CIPE that enables the MG to manage and schedule the routing of content through content filters (by MG_CIS ([SRS-7-196])) in accordance with the MG content inspection policy IEG-C_CIP_BS_EMAIL.			
SOW Annex-A	[SRS-7-17]	MG_DEX MUST offer a IPv4 and IPv6, [IETF RFC 791, 1981], and [IETF RFC 8200, 2017], over Ethernet interface 'Communications Access Services LH' on top of MG_IF_NET_LOW and MG_IF_NET_HIGH.			
SOW Annex-A	[SRS-7-170]	The design and functionality of MG_CIPE SHOULD conform to the NATO CIPE functional specification in [NC3A TN-1486, 2012].			
SOW Annex-A	[SRS-7-508]	If WG_CIPE does not conform to the NATO CIPE functional specification in [NC3A TN-1486, 2012], the proposed functional specification of the WG_CIPE SHALL be de-scribed in the bid response.			
SOW Annex-A	[SRS-7-171]	MG_CIPE SHALL ensure that no illicit information flows exist to circumvent the enforcement of MG_CIP.			
SOW Annex-A	[SRS-7-172]	MG_CIPE SHALL ensure that enforcement actions are executed in the order as specified in IEG-C_CIP_BS_EMAIL ([SRS-7-187])			
SOW Annex-A	[SRS-7-173]	For the flow of information from MG_IF_NET_HIGH to MG_IF_NET_LOW, MG_CIPE SHALL offer an interface 'CIPE Services High to Low' that accepts information for further processing.			
SOW Annex-A	[SRS-7-174]	The interface 'CIPE Services High to Low' MUST support an operation 'Enforce HL Business Support CIPE' that enforces the policy IEG-C_CIP_BS_EMAIL_HL.			
SOW Annex-A	[SRS-7-175]	The operation 'Enforce HL Business Support CIPE' MUST support the invocation of the following operations at the interface 'Content Inspection Services' ([SRS-7-204]) provided by MG_CIS ([SRS-7-196]): • Operation 'Initialize' ([SRS-7-205]) that takes as input an identifier CIPE_CF_ID that identifies a content filter in MG_CIS; • Operation 'Filter' ([SRS-7-207]) that takes as input a data object CIPE_DATA and a set of rules CIPE_DATA_RULES for processing CIPE_DATA; • Operation 'Halt' ([SRS-7-209]) that takes as input an attribute CIPE_CF_ID that identifies a content filter in MG_CIS.			
SOW Annex-A	[SRS-7-176]	MG_CIPE SHALL determine CIPE_CF_ID, CIPE_DATA and CIPE_DATA_RULES based on the policy IEG-C_CIP_BS_EMAIL_HL.			
SOW Annex-A	[SRS-7-177]	The operation 'Enforce HL Business Support CIPE' SHALL log and report the actions taken.			
SOW Annex-A	[SRS-7-178]	MG_CIPE SHALL inform MG_IFCPE of the outcome O_MG_CIPE_HL of the enforcement of IEG-C_CIP_BS_EMAIL_HL based on MG_CIP.			
SOW Annex-A	[SRS-7-179]	For the flow of information from MG_IF_NET_LOW to MG_IF_NET_HIGH, MG_CIPE MUST offer an interface 'CIPE Services Low to High' that accepts information for further processing.			
SOW Annex-A	[SRS-7-18]	The interface 'Communications Access Services LH' MUST support an operation 'ReceiveInternalNetworkLH' on top of MG_IF_NET_LOW that provides TCP/IP connectivity on the low domain by receiving IP traffic for processing by the MG.			
SOW Annex-A	[SRS-7-180]	The interface 'CIPE Services Low to High' MUST support an operation 'Enforce LH BS CIPE' that enforces the policy IEG-C_CIP_BS_EMAIL_LH.			
SOW Annex-A	[SRS-7-181]	The operation 'Enforce LH Business Support CIPE' MUST support the invocation of the following operations at the interface 'Content Inspection Services' ([SRS-7-204]) provided by MG_CIS ([SRS-7-196]): • Operation 'Initialize' ([SRS-7-205]) that takes as input an identifier CIPE_CF_ID that identifies a content filter in MG_CIS; • Operation 'Filter' ([SRS-7-207]) that takes as input a data object CIPE_DATA and a set of rules CIPE_DATA_RULES for processing CIPE_DATA; • Operation 'Halt' ([SRS-7-209]) that takes as input an attribute CIPE_CF_ID that identifies a content filter in MG_CIS.			
SOW Annex-A	[SRS-7-181]	MG_CIPE SHALL determine CIPE_CF_ID, CIPE_DATA and CIPE_DATA_RULES based on the policy IEG-C_CIP_BS_EMAIL_LH.			
SOW Annex-A	[SRS-7-183]	The operation 'Enforce LH Business Support CIPE' SHALL log and report the actions taken.			
SOW Annex-A	[SRS-7-184]	MG_CIPE SHALL inform MG_IFCPE of the outcome O_MG_CIPE_LH of the enforcement of MG_CIP_LH based on IEG-C_CIP_BS_EMAIL_LH ([SRS-7-109]).			
SOW Annex-A	[SRS-7-185]	MG_CIP SHALL be configurable.			
SOW Annex-A	[SRS-7-186]	MG_CIP SHALL specify the actions ACTIONS that need to be executed by MG_CIS.			
SOW Annex-A	[SRS-7-187]	MG_CIP SHALL specify the order in which ACTIONS need to be executed.			
SOW Annex-A	[SRS-7-188]	For each action in ACTIONS it SHALL be possible to: • Enable or disable the action. • Instruct MG_CIPE to ignore the outcome of the execution of the action by MG_CIS (as received from MG_CIS ([SRS-7-196])). • If the outcome of the execution of the action by MG_CIS is a policy violation: instruct MG_CIPE to continue the enforcement of MG_CIP, or to stop.			
SOW Annex-A	[SRS-7-189]	It SHALL be possible to group ACTIONS per the following sub-policies: • MG_CIP_EV – SMTP Envelope Validation • MG_CIP_AV – Attachment Validation • MG_CIP_LV – Label Validation			
SOW Annex-A	[SRS-7-19]	The operation 'ReceiveInternalNetworkLH' MUST support error handling as specified in [IETF RFC 7414, 2015].			
SOW Annex-A	[SRS-7-190]	MG_CIP SHALL specify the level of granularity of the outcomes O_MG_CIS ([SRS-7-205]), O_MG_CIPE_HL ([SRS-7-178]) and O_MG_CIPE_LH ([SRS-7-184]).			
SOW Annex-A	[SRS-7-191]	It SHALL be possible for MG_CIS to distinguish within O_MG_CIS, O_MG_CIPE_HL and O_MG_CIPE_LH: • The MG_CIS capability that determined a policy violation (MG_CIS_EV ([SRS-7-274]), MG_CIS_AV ([SRS-7-240]) and MG_CIS_LV ([SRS-7-214])); • Identification CIPE_CF_ID of the content filter that determined the policy violation; • Identification of the action that led to policy violation; • Reason for policy violation.			
SOW Annex-A	[SRS-7-192]	MG_CIP_EV SHALL specify the lists that are used by the Envelope Validation Content Inspection Service (MG_CIS_EV): • LIST_MG_CIS_EV_ORIG – list of allowable SMTP originators; • LIST_MG_CIS_EV_RECIPS – list of allowable SMTP recipients.			

SOW Annex-A	[SRS-7-193]	MG_CIP_AV SHALL specify the lists that are used by the Attachment Validation Content Inspection Service (MG_CIS_AV): • NUM_MG_CIS_AV_ATTACHMENTS – the maximum number of attachments; • LIST_MG_CIS_AV_TYPES – list of allowable attachment types. • LIST_MG_CIS_AV_DIRTYWORDS – list of words or phrases not allowed in an email message. • LIST_MG_CIS_AV_MALWARE_DEFINITIONS – list of definitions/signatures of currently known malware.			
SOW Annex-A	[SRS-7-194]	MG_CIP_LV SHALL specify the parameters for the Label Validation Content Inspection Service (MG_CIS_LV): • LIST_MG_CIS_LV-SPIF – list of allowable security policies (including classifications and categories); • LIST_MG_CIS_LV-DM – list of allowable digest method algorithms; • LIST_MG_CIS_LV-SM – list of allowable signature method algorithms; • LIST_MG_CIS_LV-CRL – list of certificate revocation lists • LIST_MG_CIS_LV_TP – list of trust points (e.g. trusted root certificates). • BOOL_MG_CIS_LV_CB – to indicate whether a Cryptographic Binding is required. • STR_MG_CIS_LV_FLOT_PREFIX – prefix to identify a FLOT in a message; • LIST_MG_CIS_LV_FLOT – list of valid FLOT markings; • STR_MG_CIS_LV_KEYWORD_HEADER – SMTP header field which contains keywords; • LIST_MG_CIS_LV_KEYWORDS – list of valid keywords.			
SOW Annex-A	[SRS-7-196]	The MG MUST provide a content inspection services (CIS) capability MG_CIS that enables MG_CIPE to identify and verify content based on the content inspection policy MG_CIP.			
SOW Annex-A	[SRS-7-197]	For the identification and verification of content based on MG_CIP, MG_CIS SHOULD provide a content-filter capability as specified in the NATO CIPE functional specification in [NC3A TN-1486, 2012].			
SOW Annex-A	[SRS-7-198]	MG_CIS SHALL support the message syntax of SMTP messages as defined in Simple Mail Transfer Protocol [IETF RFC 5321, 2008].			
SOW Annex-A	[SRS-7-199]	MG_CIS SHALL support XML 1.0 [W3C XML, 2006].			
SOW Annex-A	[SRS-7-2]	The MG SHALL offer a physical network interface MG_IF_NET_HIGH that provides Ethernet connectivity to the high domain.			
SOW Annex-A	[SRS-7-20]	The interface 'Communications Access Services LH' MUST support an operation 'ForwardInternalNetworkLH' on top of MG_IF_NET_HIGH that forwards IP traffic to the high domain.			
SOW Annex-A	[SRS-7-200]	MG_CIS SHALL support the XML Schema Language 1.0 [W3C XML Schema 1, 2004], [W3C XML Schema 2, 2004].			
SOW Annex-A	[SRS-7-201]	MG_CIS SHALL support Canonical XML Version 1.1 [W3X Canonical XML 1.1, 2008].			
SOW Annex-A	[SRS-7-202]	MG_CIS SHALL support XML Path Language (XPath) Version 1.0 [W3C XML Path Language 1.0, 1999].			
SOW Annex-A	[SRS-7-203]	MG_CIS SHALL support XML Pointer Language (XPointer) [W3C XPointer, 2002].			
SOW Annex-A	[SRS-7-204]	MG_CIS MUST offer an interface 'Content Inspection Services' that serves as a communication mechanism between the content filters and MG_CIPE.			
SOW Annex-A	[SRS-7-205]	The interface 'Content Inspection Services' MUST support an operation 'Initialize' that initializes a content filter.			
SOW Annex-A	[SRS-7-206]	The operation 'Initialize' MUST support the identification of a content filter based on a content filter identifier CIPE_CF_ID.			
SOW Annex-A	[SRS-7-207]	The interface 'Content Inspection Services' MUST support an operation 'Filter' that executes a content filter.			
SOW Annex-A	[SRS-7-208]	The operation 'Filter' SHALL accept as input a data object CIPE_DATA and a set of rules CIPE_DATA_RULES for processing CIPE_DATA.			
SOW Annex-A	[SRS-7-209]	The interface 'Content Inspection Services' MUST support an operation 'Halt' that halts a content filter.			
SOW Annex-A	[SRS-7-21]	The operation 'ForwardInternalNetworkLH' MUST support error handling as specified in [IETF RFC 7414, 2015].			
SOW Annex-A	[SRS-7-210]	The operation 'Halt' MUST support the identification of a content filter based on a content filter identifier CIPE_CF_ID.			
SOW Annex-A	[SRS-7-211]	MG_CIS SHALL inform MG_CIPE of the outcome O_MG_CIS of the execution of an action in ACTIONS ([SRS-7-120]).			
SOW Annex-A	[SRS-7-212]	If the outcome O_MG_CIS is negative (e.g. verification or validation fails), MG_CIS SHALL interpret O_MG_CIS as a policy violation and inform MG_CIPE according to MG_CIP ([SRS-7-185]).			
SOW Annex-A	[SRS-7-213]	MG_CIS SHALL invoke the operation 'Log' (7.7.7.1.1) at the interface 'Event Management' ([SRS-6-328]) and log the outcome O_MG_CIS ([SRS-6-115]).			
SOW Annex-A	[SRS-7-214]	MG_CIS SHALL provide a Label validation capability MG_CIS_LV.			
SOW Annex-A	[SRS-7-215]	MG_CIS_LV SHALL act upon the contents of the SMTP Message body.			
SOW Annex-A	[SRS-7-216]	MG_CIS_LV SHALL make use of the following subordinate Label validation capabilities: • MG_CIS_LV_STANAG – validation of a STANAG 4774 confidentiality label • MG_CIS_LV_FLOT – validation of a First Line of Text (FLOT) marking • MG_CIS_LV_KEYWORDS – validation of keywords.			
SOW Annex-A	[SRS-7-217]	MG_CIS_LV SHALL return a positive O_MG_CIS_LV if any of the subordinate Label validation capabilities (MG_CS_LV_STANAG, MG_CIS_LV_FLOT and MG_CIS_LV_KEYWORDS) returns a positive outcome.			
SOW Annex-A	[SRS-7-218]	The subordinate Label validation capability MG_CIS_LV_STANAG SHALL ensure that a valid and allowable STANAG 4774 confidentiality label is bound with a valid STANAG 4778 Metadata Binding to every email message.			
SOW Annex-A	[SRS-7-219]	MG_CIS_LV_STANAG MUST support the NATO standard ADatP-4774 "Confidentiality Metadata Label Syntax" [STANAG 4774].			
SOW Annex-A	[SRS-7-22]	The Business Support Service LH Interface SHALL support an operation "ReceiveEmailLH" that supports the reception of an email message from the Low Domain.			
SOW Annex-A	[SRS-7-220]	MG_CIS_LV_STANAG MUST support the NATO standard ADatP-4778 "Metadata Binding Mechanism" [STANAG 4778].			
SOW Annex-A	[SRS-7-221]	MG_CIS_LV_STANAG MUST support the binding profile "Simple Message Transport Protocol (SMTP) Binding Profile" in [STANAG 4778 SRD.2].			
SOW Annex-A	[SRS-7-222]	MG_CIS_LV_STANAG MUST support the binding profile "Cryptographic Message Syntax (CMS) Cryptographic Artefact Binding Profile" in [STANAG 4778 SRD.2].			
SOW Annex-A	[SRS-7-223]	MG_CIS_LV_STANAG SHALL be able to validate a digital signature by invoking the operation 'VerifyCMS' (7.6.2.2.1) at the interface 'Public Key Cryptographic Services' ([SRS-7-296]) provided by MG_PKCS ([SRS-7-294]).			
SOW Annex-A	[SRS-7-224]	For the confidentiality metadata labels (originator or alternative) *CLs* that are bound to a data object *DO* , MG_CIS_LV_STANAG SHALL be able to verify at least one *CL* against a security policy information file (SPIF) contained in LIST_MG_CIS_LV-SPIF.			
SOW Annex-A	[SRS-7-225]	MG_CIS_LV_STANAG SHALL be able to validate a digital signature on each SPIF contained in LIST_MG_CIS_LV-SPIF by invoking the operation 'VerifyXML' (7.6.2.2.2) at the interface 'Public Key Cryptographic Services' ([SRS7-296]) provided by MG_PKCS ([SRS-7-294]).			
SOW Annex-A	[SRS-7-226]	The subordinate Label validation capability MG_CIS_LV_FLOT SHALL ensure that a valid and allowable First Line Of Text marking is contained in every email message.			
SOW Annex-A	[SRS-7-227]	MG_CIS_LV_FLOT SHALL identify the FLOT security marking of an email message as the text following the prefix STR_MG_CIS_LV_FLOT_PREFIX on the first line of the first text attachment in the message.			
SOW Annex-A	[SRS-7-228]	The sub-policy IEG-C_CIP_BS_EMAIL_LV_FLOT SHALL determine that an email message that does not contain a FLOT security marking is non-compliant with the policy and return a negative outcome to MG_CIS_LV.			
SOW Annex-A	[SRS-7-229]	MG_CIS_LV_FLOT SHALL perform case insensitive and normalised whitespace (stripping leading and trailing white space and replacing sequences of white space characters with a single space) matching when comparing the FLOT security marking with the allowable security markings in LIST_MG_CIS_LV_FLOT			
SOW Annex-A	[SRS-7-23]	The "ReceiveEmailLH" operation SHALL be compliant with the Simple Mail Transfer Protocol (SMTP) [IETF RFC 5321, 2008].			
SOW Annex-A	[SRS-7-230]	MG_CIS_LV_FLOT SHALL determine that an email message that contains a FLOT security marking that is not an allowable security marking is non-compliant with the policy and return a negative outcome to MG_CIS_LV.			
SOW Annex-A	[SRS-7-231]	MG_CIS_LV_FLOT SHALL determine that an email message that contains a FLOT security marking that is an allowable security marking is compliant with the policy and return an positive outcome to MG_CIS_LV.			
SOW Annex-A	[SRS-7-232]	The subordinate Label validation capability MG_CIS_LV_KEYWORDS SHALL ensure that at least one valid and allowable keyword is contained in every email message.			
SOW Annex-A	[SRS-7-233]	MG_CIS_LV_KEYWORDS SHALL return a positive outcome if the list of keywords, LIST_MG_CIS_LV_KEYWORDS is empty, or the header field STR_MG_CIS_LV_KEYWORD_HEADER is empty.			
SOW Annex-A	[SRS-7-234]	MG_CIS_LV_KEYWORDS SHALL identify the KEYWORDS security marking of an email message as the text of the header field, STR_MG_CIS_LV_KEYWORD_HEADER.			
SOW Annex-A	[SRS-7-235]	The sub-policy IEG-C_CIP_BS_EMAIL_LV_ KEYWORDS SHALL split the comma-separated KEYWORDS into a list of KEYWORDs.			
SOW Annex-A	[SRS-7-236]	The sub-policy IEG-C_CIP_BS_EMAIL_LV_ KEYWORDS SHALL perform case insensitive and normalised whitespace (stripping leading and trailing white space and replacing sequences of white space characters with a single space) matching when comparing each of the KEYWORD security marking with the allowable security markings.			
SOW Annex-A	[SRS-7-237]	The sub-policy IEG-C_CIP_BS_EMAIL_LV_ KEYWORDS SHALL determine that an email message that does not contain a KEYWORDS header field is non-compliant with the policy.			
SOW Annex-A	[SRS-7-238]	The sub-policy IEG-C_CIP_BS_EMAIL_LV_ KEYWORDS SHALL determine that an email message that contains a KEYWORD security marking that is not an allowable security marking is non-compliant with the policy.			
SOW Annex-A	[SRS-7-239]	The sub-policy IEG-C_CIP_BS_EMAIL_LV_ KEYWORDS SHALL determine that an email message that contains a KEYWORD security marking that is an allowable security marking is compliant with the policy.			
SOW Annex-A	[SRS-7-24]	The "ReceiveEmailLH" operation SHALL be compliant with the SMTP Service Extension for Secure SMTP over Transport Layer Security [IETF RFC 7817, 2016].			
SOW Annex-A	[SRS-7-240]	MG_CIS SHALL provide an attachment validation capability MG_CIS_AV.			
SOW Annex-A	[SRS-7-241]	MG_CIS_AV SHALL act upon on the contents of the SMTP Message body.			
SOW Annex-A	[SRS-7-242]	MG_CIS_AV SHALL make use of the following subordinate Attachment validation capabilities: • MG_CIS_AV_MAX – validation of the maximum number of attachments; • MG_CIS_AV_TYPES – validation attachment types; • MG_CIS_AV_DIRTY – detection of dirty words; • MG_CIS_AV_MALWARE – detection of malware.			
SOW Annex-A	[SRS-7-243]	MG_CIS_AV SHALL return a positive outcome O_MG_CIS_AV only if all of the subordinate Attachment validation capabilities (MG_CS_LV_STANAG, MG_CIS_LV_FLOT and MG_CIS_LV_KEYWORDS) returns a positive outcome.			

SOW Annex-A	[SRS-7-244]	The subordinate Attachment validation capability MG_CIS_AV_MAX SHALL verify that an email message does not exceed a maximum number of attachments.			
SOW Annex-A	[SRS-7-245]	MG_CIS_AV_MAX SHALL determine the number of attachments included within a message, recursively including attachments in attached messages.			
SOW Annex-A	[SRS-7-246]	MG_CIS_AV_MAX SHALL determine that an email message that contains the configured maximum number of attachment, or less, is compliant with the policy.			
SOW Annex-A	[SRS-7-247]	MG_CIS_AV_MAX SHALL determine that an email message that contains more than the configured maximum number of attachment is non-compliant with the policy and return a negative outcome to MG_CIS_AV;			
SOW Annex-A	[SRS-7-248]	The subordinate Attachment validation capability MG_CIS_AV_TYPES SHALL ensure that an email message only contains allowed attachment types.			
SOW Annex-A	[SRS-7-249]	MG_CIS_AV_TYPES SHALL determine the *declared* media types as those contained in the Content-Type header fields, within the email message.			
SOW Annex-A	[SRS-7-25]	The "ReceiveEmailLH" operation SHALL be compliant with the SMTP Service Extension for Delivery Status Notifications [IETF RFC 3461, 2003].			
SOW Annex-A	[SRS-7-250]	MG_CIS_AV_TYPES SHALL determine the disposition media types, as derived from the filename parameter in the Content-Disposition header fields, within the email message.			
SOW Annex-A	[SRS-7-252]	MG_CIS_AV_TYPES SHALL return a positive outcome if the list of media types, LIST_MG_CIS_AV_TYPES, is empty.			
SOW Annex-A	[SRS-7-253]	MG_CIS_AV_TYPES SHALL determine an email message is compliant with the policy, if all the *disposition* media types are present in the allowed list of media types, LIST_MG_CIS_AV_TYPES.			
SOW Annex-A	[SRS-7-254]	MG_CIS_AV_TYPES SHALL determine an email message is non-compliant with the policy, if one or more the *disposition* media types are not present in the allowed list of media types, LIST_MG_CIS_AV_TYPES.			
SOW Annex-A	[SRS-7-255]	MG_CIS_AV_TYPES SHALL determine the *analysed* media types from an analysis of the contents of the email attachments.			
SOW Annex-A	[SRS-7-256]	MG_CIS_AV_TYPES SHALL determine an email message is non-compliant with the policy it is unable to determine an *analysed* media type for one or more attachments.			
SOW Annex-A	[SRS-7-257]	MG_CIS_AV_TYPES SHALL determine an email message is compliant with the policy, if all the *analysed* media types are present in the allowed list of media types, LIST_MG_CIS_AV_TYPES.			
SOW Annex-A	[SRS-7-258]	MG_CIS_AV_TYPES SHALL determine an email message is non-compliant with the policy, if one or more the *analysed* media types are not present in the allowed list of media types, LIST_MG_CIS_AV_TYPES.			
SOW Annex-A	[SRS-7-259]	The sub-policy IEG-C_CIP_BS_EMAIL_AV_TYPES SHALL determine the *container* media types (e.g. zip), as derived from the filenames and binary analysis of the files found within container email attachments.			
SOW Annex-A	[SRS-7-26]	The "ReceiveEmailLH" operation SHALL be compliant with the Extensible Message Format for Delivery Status Notifications [IETF RFC 3464, 2003].			
SOW Annex-A	[SRS-7-260]	MG_CIS_AV_TYPES SHALL determine an email message is compliant with the policy, if all the *container* media types are present in the allowed list of media types, LIST_MG_CIS_AV_TYPES.			
SOW Annex-A	[SRS-7-261]	MG_CIS_AV_TYPES SHALL determine an email message is non-compliant with the policy, if one or more the *container* media types are not present in the allowed list of media types, LIST_MG_CIS_AV_TYPES.			
SOW Annex-A	[SRS-7-262]	The subordinate Label validation capability MG_CIS_AV_DIRTY SHALL ensure an email message does not contain any of a configured set of words or phrases (LIST_MG_CIS_AV_DIRTYWORDS).			
SOW Annex-A	[SRS-7-263]	MG_CIS_AV_DIRTY SHALL return a positive outcome if the list of dirty words, LIST_MG_CIS_AV_DIRTYWORDS, is empty.			
SOW Annex-A	[SRS-7-264]	The sub-policy IEG-C_CIP_BS_EMAIL_AV_DIRTY SHALL inspect each of the email attachments, including the message body, for occurrences of any of the dirty words/phrases (LIST_MG_CIS_AV_DIRTYWORDS).			
SOW Annex-A	[SRS-7-265]	The sub-policy IEG-C_CIP_BS_EMAIL_AV_DIRTY SHALL recursively inspect each of the email message attachments for occurrences of any of the dirty words/phrases (LIST_MG_CIS_AV_DIRTYWORDS).			
SOW Annex-A	[SRS-7-266]	The sub-policy IEG-C_CIP_BS_EMAIL_AV_DIRTY SHALL perform case insensitive and normalised whitespace (stripping leading and trailing white space and replacing sequences of white space characters with a single space) matching when searching for each of the dirty words/phrases in the message body/attachment.			
SOW Annex-A	[SRS-7-267]	The sub-policy IEG-C_CIP_BS_EMAIL_AV_DIRTY SHALL determine that an email message that contains at least one of the dirty word/phrases (LIST_MG_CIS_AV_DIRTYWORDS) is non-compliant with the policy.			
SOW Annex-A	[SRS-7-268]	The sub-policy IEG-C_CIP_BS_EMAIL_AV_DIRTY SHALL determine that an email message that does not contains any of the dirty words/phrases in LIST_MG_CIS_AV_DIRTYWORDS is compliant with the policy.			
SOW Annex-A	[SRS-7-269]	The subordinate Attachment validation capability MG_CIS_AV_MALWARE SHALL ensure an email message does not contain any known malware.			
SOW Annex-A	[SRS-7-27]	The "ReceiveEmailLH" operation SHALL audit the following information for each email received: • received time; • originator; • recipients; • subject; and • message identifier.			
SOW Annex-A	[SRS-7-270]	The sub-policy IEG-C_CIP_BS_EMAIL_AV_MALWARE SHALL scan each attachment within the email message for malware using the current set of malware definitions (LIST_MG_CIS_AV_MALWARE_DEFINTIONS).			
SOW Annex-A	[SRS-7-272]	The sub-policy IEG-C_CIP_BS_EMAIL_AV_MALWARE SHALL determine that an email message that contains at least one attachment that is reported to contain malware is non-compliant with the policy.			
SOW Annex-A	[SRS-7-273]	The sub-policy IEG-C_CIP_BS_EMAIL_AV_MALWARE SHALL determine that an email message that does not contains any attachment that is reported to contain malware is compliant with the policy.			
SOW Annex-A	[SRS-7-274]	MG_CIS SHALL provide an SMTP envelope validation capability MG_CIS_EV that comprises a set of content filters.			
SOW Annex-A	[SRS-7-275]	MG_CIS_EV SHALL act upon on the contents of the SMTP message envelope.			
SOW Annex-A	[SRS-7-276]	MG_CIS_EV SHALL make use of the following subordinate SMTP envelope validation capabilities: • MG_CIS_EV_ORIG – validation of the SMTP originator; • MG_CIS_EV_RECIP – validation of the SMTP recipients;			
SOW Annex-A	[SRS-7-277]	MG_CIS_EV SHALL return a positive outcome OMG__CIS_EV only if all of the subordinate Envelope validation capabilities (MG_CS_EV_ORIG and MG_CIS_EV_RECIP) return a positive outcome.			
SOW Annex-A	[SRS-7-278]	The subordinate SMTP envelope validation capability, MG_CIS_EV_ORIG, SHALL allow the configuration of a set of allowable message originators, LIST_MG_CIS_EV_ORIG, one of which a compliant email message must contain.			
SOW Annex-A	[SRS-7-279]	MG_CIS_EV_ORIG SHALL allow a configured message originator to contain wildcards in the local-part of the address.			
SOW Annex-A	[SRS-7-28]	The Business Support Service LH Interface SHALL support an operation "ForwardEmailLH" that supports the transfer of an email message to the low domain.			
SOW Annex-A	[SRS-7-280]	MG_CIS_EV_ORIG SHALL allow a configured message originator to contain wildcards in the domain components of the address.			
SOW Annex-A	[SRS-7-281]	MG_CIS_EV_ORIG SHALL identify the email message originator as the MAIL FROM: field as defined in [IETF RFC 5321, 2008].			
SOW Annex-A	[SRS-7-282]	MG_CIS_EV_ORIG SHALL perform case insensitive matching when comparing the email message originator with the allowable message originators.			
SOW Annex-A	[SRS-7-283]	MG_CIS_EV_ORIG SHALL take into account the wildcards when comparing the email message originator with the allowable message originators.			
SOW Annex-A	[SRS-7-284]	MG_CIS_EV_ORIG SHALL determine that an email message that contains an email message originator that is not an allowable message originator is non-compliant with the policy.			
SOW Annex-A	[SRS-7-285]	MG_CIS_EV_ORIG SHALL determine that an email message that contains an originator that is an allowable message originator is compliant with the policy.			
SOW Annex-A	[SRS-7-286]	The subordinate SMTP envelope validation capability, MG_CIS_EV_RECIP, SHALL allow the configuration of a set of allowable message recipients that a compliant email message may contain.			
SOW Annex-A	[SRS-7-287]	MG_CIS_EV_RECIP SHALL allow a message recipient to contain wildcards in the local-part of the address.			
SOW Annex-A	[SRS-7-288]	MG_CIS_EV_RECIP SHALL allow a message recipient to contain wildcards in the domain components of the address.			
SOW Annex-A	[SRS-7-289]	MG_CIS_EV_RECIP SHALL identify the email message originator as the RCPT TO: field as defined in [IETF RFC 5321, 2008].			
SOW Annex-A	[SRS-7-29]	The "ForwardEmailLH" operation SHALL be compliant with the Simple Mail Transfer Protocol (SMTP) [IETF RFC 5321, 2008].			
SOW Annex-A	[SRS-7-290]	MG_CIS_EV_RECIP SHALL perform case insensitive matching when comparing the email message recipient with the allowable message recipients.			
SOW Annex-A	[SRS-7-291]	MG_CIS_EV_RECIP SHALL take into the wildcards when comparing the email message originator with the allowable message originators.			
SOW Annex-A	[SRS-7-292]	MG_CIS_EV_RECIP SHALL determine that an email message that contains an email message recipient that is not an allowable message recipient is non-compliant with the policy.			
SOW Annex-A	[SRS-7-293]	MG_CIS_EV_RECIP SHALL determine that an email message that contains a recipient that is an allowable message recipient is compliant with the policy.			
SOW Annex-A	[SRS-7-294]	MG MUST provide a capability MG_PKCS that enables the MG to perform cryptographic operations and key management.			
SOW Annex-A	[SRS-7-295]	MG_PKCS SHALL conform to the INFOSEC Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanisms [NAC AC/322-D/0047-REV2 (INV)].			
SOW Annex-A	[SRS-7-296]	MG_PKCS MUST offer an interface 'Public Key Cryptographic Services' that supports the following cryptographic operations: • VerifyCMS (7.6.2.2.1); • VerifyXML (7.6.2.2.2); • Encrypt (7.6.2.2.3); • Decrypt (7.6.2.2.4).			
SOW Annex-A	[SRS-7-297]	For every action taken, the operations 'VerifyCMS, 'VerifyXML', 'Encrypt' and 'Decrypt' SHALL invoke the operation 'Log' (6.7.7.2.2) at the interface 'Event Management' ([SRS-6-328]) and log both the action and the result of the action.			

SOW Annex-A	[SRS-7-298]	The operation 'VerifyCMS': • MUST support the validation of Cryptographic Message Syntax SignedData digital signatures based on the Cryptographic Message Syntax ([IETF RFC 5652, 2009]); • MUST support validation of digital signatures in accordance with a specified cryptographic algorithm: the Rivest Shamir Adleman (RSA) algorithm [RSA PKCS#1, 2002] and cryptographic key sizes of 3072 bits that meet the following: o Requirements defined in the NPKI Certificate Policy [NAC AC/322-D(2004)0024 REV3-COR1, 2018] and [NAC AC/322-D(2007)0002-REV1, 2015]			
SOW Annex-A	[SRS-7-299]	The operation 'VerifyXML': • MUST support the validation of XML digital signatures based on XMLDSIG Core Validation [W3C XMLDSIG-CORE, 2008]; • MUST support validation of XML digital signatures in accordance with a specified cryptographic algorithm: the Rivest Shamir Adleman (RSA) algorithm [RSA PKCS#1, 2002] and cryptographic key sizes of 3072 bits that meet the following: o Requirements defined in the NPKI Certificate Policy [NAC AC/322-D(2004)0024-REV3-COR1, 2018] and [NAC AC/322-D(2007)0002-REV1, 2015] o The XML Signature Syntax and Processing standard (Second Edition) [W3C XMLDsig-2nd-Ed, 2008]. • MUST support signatures of the types XMLDSIG 'enveloping' and 'enveloped'. • MAY support signatures of the type XMLDSIG 'detached'. • MUST support the validation and of cryptographic bindings according to 'Cryptographic Artefact Binding Profiles' [STANAG 4778 SRD.2].			
SOW Annex-A	[SRS-7-3]	MG_IF_NET_HIGH SHALL support an operation 'ReceiveHigh' that receives (transfer-in) data from the high domain for processing by the MG.			
SOW Annex-A	[SRS-7-30]	The "ForwardEmailLH" operation SHALL be compliant with the Internet Message Format [IETF RFC 5322, 2008].			
SOW Annex-A	[SRS-7-300]	The operation 'Encrypt' MUST support encryption of data conformant with Transport Layer Security (TLS, [IETF RFC 8446, 2018]).			
SOW Annex-A	[SRS-7-301]	The operation 'Decrypt' MUST support decryption of data conformant with Transport Layer Security (TLS, [IETF RFC 8446, 2018]).			
SOW Annex-A	[SRS-7-302]	The MG MUST provide a management capability MG_MGMT that supports local and remote management of the MG.			
SOW Annex-A	[SRS-7-303]	For local management, MG_MGMT MUST offer an interface MG_IF_LOCAL_MGMT consisting of a directly attached keyboard and display console.			
SOW Annex-A	[SRS-7-304]	MG_IF_LOCAL_MGMT SHALL support the invocation of the operations at the interfaces 'CIS Security' ([SRS-7-331]), 'SMC Configuration Management' ([SRS-7-352]) and 'Cyber Defence' 7.7.6).			
SOW Annex-A	[SRS-7-305]	MG_MGMT MUST provide a capability MG_MGMT_AM that allows Audit Administrators to fulfil their role.			
SOW Annex-A	[SRS-7-306]	MG_MGMT_AM MUST be interoperable with NATO auditing and system management tools.			
SOW Annex-A	[SRS-7-307]	MG_MGMT_AM SHALL provide the capability to detect and create records of security-relevant events associated with users.			
SOW Annex-A	[SRS-7-308]	MG_MGMT_AM SHALL provide the capability to detect and create records of security-relevant events associated with end users transferring messages cross domain.			
SOW Annex-A	[SRS-7-309]	MG_MGMT_AM SHALL provide the capability to appropriately classify and protect audit information in accordance with NATO security policy.			
SOW Annex-A	[SRS-7-31]	The "ForwardEmailLH" operation SHALL be compliant with the SMTP Service Extension for Secure SMTP over Transport Layer Security [IETF RFC 7817, 2016].			
SOW Annex-A	[SRS-7-310]	MG_MGMT_AM SHALL provide mechanisms to protect audit logs from unauthorised access, modification and deletion.			
SOW Annex-A	[SRS-7-311	MG_MGMT_AM SHALL provide the capability to selectively view audit information, and alert the Audit Administrator of identified potential security violations.			
SOW Annex-A	[SRS-7-312]	MG_MGMT_AM SHALL provide reliable time stamps and the capability for the Audit Administrator to set the time used for these time stamps.			
SOW Annex-A	[SRS-7-313]	MG_MGMT_AM SHALL support the generation of an audit log for each of the following general auditable events: • MG start-up and shutdown; • Changes to security related system management functions; • Audit log access; • Creation, modification or deletion of audit log records; • Invocation of privileged operations; • Modification to MG access rights; • Unauthorised attempts to access MG system files; • All modified objects are recorded with date, time, details of change and user.			
SOW Annex-A	[SRS-7-314]	MG_MGMT_AM SHALL support the generation of an audit log for each of the following Data Exchange Services auditable events: • Data Exchange Services start-up and shutdown; • Unauthorised attempts to request access to information cross domain; • Unauthorised attempts to modify Data Exchange Services configuration; • Failed Data Exchange Services operations.			
SOW Annex-A	[SRS-7-315]	MG_MGMT_AM SHALL support the generation of an audit log for each of the following Protection Services auditable events: • Protection Services start-up and shutdown; • Failed Protection Services operations; • Unauthorised attempts to modify Protection Services configuration; • Creation, modification and deletion of Public Key Cryptographic Services keying material; • Updates of Content Inspection Services content filters; • Failed certificate path validation and revocation.			
SOW Annex-A	[SRS-7-316]	MG_MGMT_AM SHALL support the generation of an audit log for each of the following Protection Policy Enforcement Services auditable events: • Protection Policy Enforcement Services start-up and shutdown; • Failed Protection Policy Enforcement Services operations; • Unauthorised attempts to create, modify or delete Information Flow Control policies; • Unauthorised attempts to create, modify or delete Content Inspection policies.			
SOW Annex-A	[SRS-7-317]	MG_MGMT_AM SHALL support the archiving of the audit log after a period of time as configured by the Audit Administrator.			
SOW Annex-A	[SRS-7-318]	MG_MGMT_AM SHALL by default archive the audit log daily.			
SOW Annex-A	[SRS-7-319]	MG_MGMT_AM SHALL automatically back up audit logs at configurable intervals.			
SOW Annex-A	[SRS-7-32]	The "ForwardEmailLH" operation SHALL be compliant with the SMTP Service Extension for Delivery Status Notifications [IETF RFC 3461, 2003].			
SOW Annex-A	[SRS-7-320]	MG_MGMT_AM SHALL provide the capability, including integrity checking, to verify that the audit log has been archived correctly.			
SOW Annex-A	[SRS-7-321]	MG_MGMT_AM SHALL provide the capability to alert the Audit Administrator when the audit log exceeds a configurable percentage of the configurable maximum permitted size.			
SOW Annex-A	[SRS-7-322]	MG_MGMT_AM SHALL by default set the configurable percentage to 90% of the configurable maximum permitted size.			
SOW Annex-A	[SRS-7-323]	MG_MGMT SHALL provide a capability MG_MGMT_CS that allows for the management of CIS Security information specific to the MG.			
SOW Annex-A	[SRS-7-324]	MG_MGMT_CS SHALL support the retrieval of key material, certificates and CRLs from locations external to the MG.			
SOW Annex-A	[SRS-7-325]	MG_MGMT_CS SHALL validate certificates against CRLs in accordance with the NPKI Certificate Policy [NAC AC/322-D(2004)0024-REV3-COR1, 2018].			
SOW Annex-A	[SRS-7-326]	MG_MGMT_CS SHALL only trust certificates that: • Are validated using OCSP or • Can be validated to an installed trusted certificate.			
SOW Annex-A	[SRS-7-327]	MG_MGMT_CS SHALL allow the installation of multiple trusted certificates.			
SOW Annex-A	[SRS-7-328]	MG_MGMT_CS SHALL support automated execution of the following actions: • Updating of certificates; • Updating of CRLs;			
SOW Annex-A	[SRS-7-329]	MG_MGMT_CS MUST support scheduling of each operation in [SRS-7-328] such that: • The operation will be executed at a configurable date and time, with: o date expressed in years, month and day; o time expressed in hours and minutes. • When starting at a configurable date and time, the operation will be executed at a configurable regular time interval expressed in days, weeks or months.			
SOW Annex-A	[SRS-7-33]	The "ForwardEmailLH" operation SHALL be compliant with the Extensible Message Format for Delivery Status Notifications [IETF RFC 3464, 2003].			
SOW Annex-A	[SRS-7-330]	MG_MGMT_CS SHALL pass outgoing CIS Security Messages to the interface 'Core Services Management' ([SRS-7-60]) for further processing.			
SOW Annex-A	[SRS-7-331]	MG_MGMT_CS MUST offer an interface 'CIS Security' that accepts an incoming 'CIS Security Message' in support of the operations 'Manage Protection Policies' (7.7.4.1.1), 'Review' (7.7.4.1.2) and 'Manage Public Key Material' (7.7.4.1.3).			
SOW Annex-A	[SRS-7-332]	The interface 'CIS Security' MUST support an operation 'Manage Protection Policies' that provides the capability to manage the lifecycle of the IFPs and CIPs in support of MG_IFCPE ([SRS-7-82] and MG_CIPE ([SRS-7-169] respectively.			

SOW Annex-A	[SRS-7-333]	The operation 'Manage Protection Policies' SHALL support the following actions: • Create policy; • Read policy; • Update policy; • Delete policy; • Activate policy; • De-activate policy; • Backup policy; • Restore policy.			
SOW Annex-A	[SRS-7-334]	MG_MGMT_CS MUST support the automated execution of those operations in [SRS-=7-333] that comprise a policy update.			
SOW Annex-A	[SRS-7-335]	MG_MGMT_CS MUST support the automated execution of the operation 'Backup policy' in [SRS-7-333].			
SOW Annex-A	[SRS-7-336]	MG_MGMT_CS MUST support scheduling of policy updates such that: • The policy update will be executed at a configurable date and time, with: o date expressed in years, month and day; o time expressed in hours and minutes. • When starting at a configurable date and time, the policy update will be executed at a configurable regular time interval expressed in days, weeks or months.			
SOW Annex-A	[SRS-7-337]	The interface 'CIS Security' MUST support an operation 'Review' that provides the capability to review audit logs.			
SOW Annex-A	[SRS-7-338]	The interface 'CIS Security' MUST support an operation 'Manage Public Key Material' that provides the capability to manage key material to support MG_PKCS ([SRS-7-294]).			
SOW Annex-A	[SRS-7-339]	The operation 'Manage Public Key Material' SHALL be compliant with CIS Security Technical and Implementation Guidance in Support of Public Key Infrastructure – Cryptographic Artefacts [NAC AC/322-D(2007)0002-REV1, 2015].			
SOW Annex-A	[SRS-7-34]	The 'ForwardEmailLH" operation SHALL be configurable to determine the destination host of a recipient from either DNS MX records or local configuration.			
SOW Annex-A	[SRS-7-340]	The operation 'Manage Public Key Material' MUST provide the capability to: • Import and store key material; • Install and de-install certificates; • Update certificates; • Import and update CRLs.			
SOW Annex-A	[SRS-7-341]	MG_MGMT MUST provide a management capability MG_MGMT_CM that enables the configuration and management of the MG.			
SOW Annex-A	[SRS-7-342]	MG_MGMT_CM MUST provide the capability to change, capture, duplicate, backup or restore the configuration of the MG.			
SOW Annex-A	[SRS-7-343]	MG_MGMT_CM MUST provide the capability to remotely prepare a MG configuration MG_CONFIG and deploy MG_CONFIG onto multiple instances of the MG.			
SOW Annex-A	[SRS-7-344]	MG_MGMT_CM MUST offer a graphical user interface for all configuration and installation options, including the updating of XML artefacts.			
SOW Annex-A	[SRS-7-345]	MG_MGMT_CM MUST support configuration of the MG based on a customizable (pre-loaded) configuration templates (e.g. SPIFs are pre-installed) in support of common information exchange scenarios.			
SOW Annex-A	[SRS-7-346]	MG_MGMT_CM MUST support the creation and installation (pre-loading) of the configuration templates.			
SOW Annex-A	[SRS-7-347]	MG_MGMT_CM MUST support the retrieval of XML artefacts from locations external to the MG.			
SOW Annex-A	[SRS-7-348]	MG_MGMT_CM MUST support one or more of the following management protocols and associated SMC Messages for the retrieval of XML artefacts: • Secure LDAP (LDAPS) [IETF RFC 4510 – 4519, 2006]; • HTTP(S) ([IETF RFC 7230, 2014], [IETF RFC 7540, 2015] [IETF RFC 8446, 2008], [IETF RFC 2818, 2000]; • SOAP ([W3C SOAP 1.1, 2000] and [W3C SOAP 1.2, 2007]).			
SOW Annex-A	[SRS-7-349]	MG_MGMT_CM MUST support automated execution of the following action: • Updating of XML artefacts including SPIFs.			
SOW Annex-A	[SRS-7-35]	The local configuration of the destination hosts for the 'ForwardEmailLH" operation SHALL allow the use of wildcards in the domain name.			
SOW Annex-A	[SRS-7-350]	MG_MGMT_CM MUST support scheduling of the operation in [SRS-7-349] such that: • The operation will be executed at a configurable date and time, with: • date expressed in years, month and day; • time expressed in hours and minutes. • When starting at a configurable date and time, the operation will be executed at a configurable regular time interval expressed in days, weeks or months.			
SOW Annex-A	[SRS-7-351]	MG_MGMT_CM SHALL pass outgoing SMC Messages to the interface 'Core Services Management' ([SRS-7-60]) for further processing.			
SOW Annex-A	[SRS-7-352]	MG_MGMT_CM MUST offer an interface 'SMC Configuration Management' that accepts an incoming 'SMC Message' in support of the operations 'Configure OS' (7.7.5.1.1), 'Configure Protection Policy Enforcement Services" (7.7.5.1.2), 'Configure Data Exchange Services' (7.7.5.1.3) and 'Configure Protection Services' (7.7.5.1.4).			
SOW Annex-A	[SRS-7-353]	The interface 'SMC Configuration Management' MUST support an operation 'Configure OS' that provides the ability to configure and manage the operating system(s) and platform(s) the MG is running on, and the applications running on the operating system.			
SOW Annex-A	[SRS-7-354]	The operation 'Configure OS' SHALL support SMC Messages of the following types: • Secure Shell (SSH, [IETF RFC 4253, 2006]); • Network Time Protocol (NTP, [IETF RFC 5905, 2010]); • Intelligent Platform Management Interface (IPMI, [IPMI V2.0, 2013]); • Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]).			
SOW Annex-A	[SRS-7-355]	The interface 'SMC Configuration Management' MUST support an operation 'Configure Protection Policy Enforcement Services' that provides the capability to configure and manage MG_IFCPE (7.5.1.1) and MG_CIPE (7.5.3.1).			
SOW Annex-A	[SRS-7-356]	The operation 'Configure Protection Policy Enforcement Services' MUST provide the capability to change, capture, duplicate, backup or restore the configuration of MG_IFCPE and MG_CIPE.			
SOW Annex-A	[SRS-7-357]	The operation 'Configure Protection Policy Enforcement Services' SHALL support one or more SMC Messages of the following types: • Secure Shell (SSH, [IETF RFC 4253, 2006]); • Remote Desktop Protocol (RDP); • Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]).			
SOW Annex-A	[SRS-7-358]	The interface 'SMC Configuration Management' MUST support an operation 'Configure Data Exchange Services' that provides the capability to configure and manage MG_DEX ([SRS-7-1]).			
SOW Annex-A	[SRS-7-359]	The operation 'Configure Data Exchange Services' MUST provide the capability to change, capture, duplicate, backup or restore the configuration of MG_DEX.			
SOW Annex-A	[SRS-7-36]	The "ForwardEmailLH" operation SHALL allow the use the best match when determining the destination host from local configuration.			
SOW Annex-A	[SRS-7-360]	The operation 'Configure Data Exchange Services' SHALL support SMC Messages of the following types: • Secure Shell (SSH, [IETF RFC 4253, 2006]); • Remote Desktop Protocol (RDP); • Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]).			
SOW Annex-A	[SRS-7-361]	The interface 'SMC Configuration Management' MUST support an operation 'Configure Protection Services' that provides the capability to configure and manage MG_CIS ([SRS-7-196]) and MG_PKCS ([SRS-7-294]).			
SOW Annex-A	[SRS-7-362]	The operation 'Configure Protection Services' MUST provide the capability to change, capture, duplicate, backup or restore the configuration of MG_CIS and MG_PKCS.			
SOW Annex-A	[SRS-7-363]	The operation 'Configure Protection Services' SHALL support SMC Messages of the following types: • Secure Shell (SSH, [IETF RFC 4253, 2006]); • Remote Desktop Protocol (RDP); • Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]).			
SOW Annex-A	[SRS-7-364]	The operation 'Configure Protection Services' MUST provide the capability to manage filters for MG_CIS.			
SOW Annex-A	[SRS-7-365]	The management of filters for MG_CIS SHALL include: • Installation and de-installation of content filters; • Updating of content filters.			
SOW Annex-A	[SRS-7-366]	The management of XML artefacts for MG_CIS SHALL include: • Loading and removal; • Validation against the corresponding XML Schema, • Validation of any contained XML Digital Signature.			
SOW Annex-A	[SRS-7-367]	MG_MGMT MUST provide a management capability MG_MGMT_CD that provides the capability to manage and respond to cyber-related attacks on the MG.			
SOW Annex-A	[SRS-7-368]	MG_MGMT_CD SHALL pass outgoing Cyber Defence Messages to interface 'Core Services Management' ([SRS-7-60]) for further processing.			
SOW Annex-A	[SRS-7-369]	MG_MGMT_CD MUST offer an interface 'Cyber Defence' that accepts an incoming 'Cyber Defence Message' in support of the operations 'Assess' (7.7.6.1.1), 'Respond' (7.7.6.1.2) and 'Recover' (7.7.6.1.3).			
SOW Annex-A	[SRS-7-37]	The "ForwardEmailLH" operation SHALL be able to rewrite the originator and recipient email addresses in both the Simple Mail Transfer Protocol and the Internet Message Format.			
SOW Annex-A	[SRS-7-370]	The interface 'Cyber Defence' MUST support an operation 'Assess' that provides the capability to assess damage and attacks/faults of MG components that have been affected by attacks and faults.			
SOW Annex-A	[SRS-7-371]	The operation 'Assess' SHALL be able to support analysis and evaluation of an attack.			

SOW Annex-A	[SRS-7-372]	The operation 'Assess' SHALL be able to support the aggregation of cyber-related data (e.g. logs from MG_IFCPE, MG_CIPE and MG_PKCS) to a central repository to facilitate proper analysis.			
SOW Annex-A	[SRS-7-373]	The interface 'Cyber Defence' MUST support an operation 'Respond' that provides the capability to dynamically mitigate the risk identified by a suspected attack/fault.			
SOW Annex-A	[SRS-7-374]	The operation 'Respond' SHALL be able to support the controlling of traffic flows for the purpose of stopping or mitigating an attack or fault.			
SOW Annex-A	[SRS-7-375]	The controlling of traffic flow by MG_MGMT_CD SHALL include: • Termination; • Throttling to a certain level of bandwidth or with a certain delay; • Redirection.			
SOW Annex-A	[SRS-7-376]	The interface 'Cyber Defence' MUST support an operation 'Recover' that provides the capability to take the required action to recover from an attack/fault and restore the components of the MG that were affected by the attack/fault.			
SOW Annex-A	[SRS-7-377]	MG_MGMT MUST provide a management capability MG_MGMT_EM that enables the management of events.			
SOW Annex-A	[SRS-7-378]	MG_MGMT_EM SHALL collect events and support the forwarding of events to the EMS.			
SOW Annex-A	[SRS-7-379]	MG_MGMT_EM SHOULD support monitoring based on the Microsoft System Center Operations Manager (SCOM).			
SOW Annex-A	[SRS-7-38]	The "ForwardEmailLH" address rewriting SHALL allow the rewriting of both the local-part and the domain components of the email address.			
SOW Annex-A	[SRS-7-380]	MG_MGMT_EM SHALL support SNMP v3 [IETF RFC 3412, 2002] and the Mail Monitoring MIB [IETF RFC 2789, 2000]			
SOW Annex-A	[SRS-7-381]	MG_MGMT_EM SHALL provide a toolset which allows MG Administrators to define, filter, correlate and group events according to their context, criticality, source and impacts.			
SOW Annex-A	[SRS-7-382]	MG_MGMT_EM SHALL provide an event correlation toolset that can be either customizable or adaptive to detect normal and abnormal behaviour patterns.			
SOW Annex-A	[SRS-7-383]	MG_MGMT_EM SHALL provide the capability to examine recorded historical logs and archives.			
SOW Annex-A	[SRS-7-384]	MG_MGMT_EM SHALL support the correlation of requests and responses in order to track all responses (or faults) with the correct request for information access.			
SOW Annex-A	[SRS-7-386]	MG_MGMT_EM SHALL provide an event management toolset which allows MG Administrators to customize the building and saving of reports.			
SOW Annex-A	[SRS-7-387]	The event management toolset SHALL support the provision of visibility on usage patterns over daily, monthly and variable periods.			
SOW Annex-A	[SRS-7-388]	The event management toolset SHALL support trend and abnormal behaviour analysis.			
SOW Annex-A	[SRS-7-389]	MG_MGMT_EM SHALL be able to generate reports of the following types: • SLA compliance reports; • Error/exception reports; • Service usage reports;			
SOW Annex-A	[SRS-7-39]	The Business Support Service LH Interface SHALL support an operation "ReceiveEmailHL" that supports the reception of an email message from the high domain.			
SOW Annex-A	[SRS-7-390]	Other customizable reports based on captured metrics which can be filtered and sorted based on various criteria.			
SOW Annex-A	[SRS-7-391]	MG_MGMT_EM SHALL pass outgoing SMC Messages to interface 'Core Services Management' ([SRS-7-60]) for further processing.			
SOW Annex-A	[SRS-7-392]	MG_MGMT_EM MUST offer an interface 'Event Management' that generates and forwards 'SMC Messages' in support of the operations 'Log' (7.7.7.1.1), 'Alert' (7.7.7.1.2) and 'Report' (7.7.7.1.3).			
SOW Annex-A	[SRS-7-393]	The interface 'Event Management' MUST support an operation 'Log' that provides the capability to record events that occur in software, or messages between components.			
SOW Annex-A	[SRS-7-394]	The operation 'Log' SHALL support writing log messages to a log file.			
SOW Annex-A	[SRS-7-395]	The operation 'Log' MUST provide the capability to log request and response attributes. These include: • Time-stamp; • Source and target address(es); • URL; • Operation; • Size; • Unique request id (extracted from the request/response or automatically generated by MG_MGMT_EM).			
SOW Annex-A	[SRS-7-396]	The operation 'Log' MUST provide the capability to log attributes extracted from the SMTP headers and SMTP body.			
SOW Annex-A	[SRS-7-397]	The operation 'Log' MUST provide the capability to selectively log whole messages based on pre-configured criteria or filter (e.g. policy based).			
SOW Annex-A	[SRS-7-398]	The operation 'Log' SHALL support one or more SMC Messages of the following types: • Syslog [IETF RFC 5424, 2009]; • HTTP Message [IETF RFC 7230, 2014].			
SOW Annex-A	[SRS-7-399]	The interface 'Event Management' MUST support an operation 'Alert' that provides the capability to generate an alert event when the acceptable threshold for a service has been reached, or is approached within a certain range.			
SOW Annex-A	[SRS-7-4]	MG_IF_NET_HIGH SHALL support an operation 'ForwardHigh' that forwards (transfer-out) data that has been processed by the MG to the high domain.			
SOW Annex-A	[SRS-7-40]	The "ReceiveEmailHL" operation SHALL be compliant with the Simple Mail Transfer Protocol (SMTP) [IETF RFC 5321, 2008].			
SOW Annex-A	[SRS-7-400]	The operation 'Alert' SHALL be able to support the generation of an alert of type 'Warning' that indicates it is necessary to take action in order to prevent an exception occurring.			
SOW Annex-A	[SRS-7-401]	The operation 'Alert' SHALL be able to support the generation of an alert of type 'Exception' that indicates that a given service is operating below the normal predefined parameters/indicators.			
SOW Annex-A	[SRS-7-402]	The operation 'Alert' SHALL support SMC Messages of the type SNMP v3 [IETF RFC, 3412, 2002].			
SOW Annex-A	[SRS-7-403]	The interface 'Event Management' MUST support an operation 'Report' that provides the capability to generate reports in support of compliance, auditing, billing and service value determination.			
SOW Annex-A	[SRS-7-404]	The operation 'Report' SHALL support SMC Messages of the type SNMP v3 [IETF RFC 3412, 2002].			
SOW Annex-A	[SRS-7-405]	MG_MGMT MUST provide a management capability MG_MGMT_PM that enables the management of the performance and capacity of the MG.			
SOW Annex-A	[SRS-7-406]	MG_MGMT_PM SHALL provide customizable dashboards for monitoring selected statistics and metrics for MG services.			
SOW Annex-A	[SRS-7-407]	MG_MGMT_PM SHALL pass outgoing SMC Messages to interface 'Core Services Management' ([SRS-7-60] for further processing.			
SOW Annex-A	[SRS-7-408]	MG_MGMT_PM MUST offer an interface 'Performance Management' that generates and forwards 'SMC Messages' in support of the operations 'Monitor'(7.7.8.1.1), 'Meter' (7.7.8.1.2) and 'Track Messages' (7.7.8.1.3.			
SOW Annex-A	[SRS-7-409]	The interface 'Performance Management' MUST support an operation 'Monitor' that provides the capability to observe and track the operations and activities of end users (services) on the MG.			
SOW Annex-A	[SRS-7-41]	The "ReceiveEmailHL" operation SHALL be compliant with the SMTP Service Extension for Secure SMTP over Transport Layer Security [IETF RFC 7817, 2016].			
SOW Annex-A	[SRS-7-410]	The operation 'Monitor' SHALL support the real-time monitoring of MG services against expected KPI, SLA or other metric thresholds as configured.			
SOW Annex-A	[SRS-7-411]	The operation 'Monitor' SHALL support the monitoring service faults and exceptions.			
SOW Annex-A	[SRS-7-412]	The operation 'Monitor' SHALL support SMC Messages of the type SNMP v3 [IETF RFC 3412, 2002].			
SOW Annex-A	[SRS-7-413]	The interface 'Performance Management' MUST support an operation 'Meter' that provides the capability to measure levels of resource utilization consumed by service subscribers.			
SOW Annex-A	[SRS-7-414]	The operation 'Meter' SHALL support the storing of measured data for the purpose of summarizing and analysis.			
SOW Annex-A	[SRS-7-415]	The operation 'Meter' SHALL provide the capability to collect and present the statistics on service utilisation broken down by end user or system.			
SOW Annex-A	[SRS-7-416]	The operation 'Meter' SHALL support the collection of statistics for a given end user or system or group of end user or system over specified periods of time.			
SOW Annex-A	[SRS-7-417]	The operation 'Meter' SHALL support SMC Messages of the type SNMP v3 [IETF RFC 3412, 2002].			
SOW Annex-A	[SRS-7-418]	The interface 'Performance Management' MUST support an operation 'Track Messages' that provides the capability to track, monitor and log all message routing and service invocation activities.			
SOW Annex-A	[SRS-7-419]	The operation 'Track Messages' SHALL provide the capability to track, monitor, and log all SMTP messages from the high domain to the low domain.			
SOW Annex-A	[SRS-7-42]	The "ReceiveEmailHL" operation SHALL be compliant with the SMTP Service Extension for Delivery Status Notifications [IETF RFC 3461, 2003].			
SOW Annex-A	[SRS-7-420]	The operation 'Track Messages' SHALL provide the capability to track, monitor, and log all delivery reports and status notifications from the low domain to the high domain.			
SOW Annex-A	[SRS-7-421]	The operation 'Track Messages' SHALL provide the capability to track, monitor, and log all SMTP messages from the low domain to the high domain.			
SOW Annex-A	[SRS-7-422]	The operation 'Track Messages' SHALL provide the capability to track, monitor, and log all delivery reports and status notifications from the high domain to the high domain.			
SOW Annex-A	[SRS-7-423]	The operation 'Track Messages' SHALL support SMC Messages of the type SNMP v3 [IETF RFC 3412, 2002].			
SOW Annex-A	[SRS-7-424]	The MG SHALL be evaluated to EAL4(+) based on the Protection Profile defined in Section 8.			
SOW Annex-A	[SRS-7-425]	The MG SHALL include malware/virus protection for its server.			
SOW Annex-A	[SRS-7-426]	The MG malware/virus protection SHALL be maintained/updated from the NATO Service Operation Centre (SOC).			
SOW Annex-A	[SRS-7-428]	The MG SHALL protect components and areas of main memory from being directly accessed (without that access being mediated by the operating system) by untrusted subjects.			
SOW Annex-A	[SRS-7-429]	The MG SHALL protect any other function of the underlying platform from being used by untrusted subjects in a way that would violate the security policy of the operating system.			
SOW Annex-A	[SRS-7-43]	The "ReceiveEmailHL" operation SHALL be compliant with the Extensible Message Format for Delivery Status Notifications [IETF RFC 3464, 2003].			

SOW Annex-A	[SRS-7-430]	The MG SHALL provide mechanisms that control a user's logical access to the Mail Guard and to explicitly deny access to specific users when appropriate.			
SOW Annex-A	[SRS-7-431]	The MG SHALL be capable of maintaining protection policy enforcement if it is unable to communicate with the Policy Enforcement module which provided it the policy.			
SOW Annex-A	[SRS-7-432]	The MG SHALL enable the enforcement of information flows email messages.			
SOW Annex-A	[SRS-7-433]	The MG SHALL enable the enforcement of content inspection of email messages.			
SOW Annex-A	[SRS-7-434]	The MG SHALL validate the origin, integrity and binding [STANAG 4778] of a confidentiality label [STANAG 4774] to a data object before it is used.			
SOW Annex-A	[SRS-7-435]	The MG Data Protection Module SHALL provide a NATO approved cryptographic sub-component with NATO-approved methods for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys), and for cryptographic operations (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services) as described in [NAC AC/322-D(2007)0002-REV1, 2015].			
SOW Annex-A	[SRS-7-436]	The MG Data Protection Module cryptographic sub-component SHALL be validated to at least FIPS 140-2 Level 2 [FIPS 140-2, 2001], or otherwise verified to an equivalent level of functionality and assurance by a NATO nation COMSEC authority.			
SOW Annex-A	[SRS-7-437]	The MG Data Protection Module SHALL provide capability to protect against disclosing or transmitting information in violation of the policy.			
SOW Annex-A	[SRS-7-438]	The MG SHALL provide mechanisms that mitigate attempts to exhaust its resources.			
SOW Annex-A	[SRS-7-439]	The MG Data Protection Module SHALL provide capability to protect against gaining inappropriate access to one or more networks, endpoints, or services, such as through transmitting malicious executable code, scripts, or commands.			
SOW Annex-A	[SRS-7-44]	The Business Support Service HL Interface SHALL support an operation "ForwardEmailLH" that supports the transfer of an email message to the high domain.			
SOW Annex-A	[SRS-7-440]	The MG SHALL ensure that is protection policy information is transmitted to the Policy Enforcement Module in a secure and timely manner so that there is assurance that the correct policy is being enforced.			
SOW Annex-A	[SRS-7-441]	The MG SHALL ensure that communications are not subject to unauthorized modification or disclosure.			
SOW Annex-A	[SRS-7-442]	The MG SHALL provide a means to ensure that administrators are not communicating with some other entity pretending to be the MG when supplying identification and authentication data.			
SOW Annex-A	[SRS-7-443]	The MG SHALL validate the identity of other peer entities prior to distributing data to them.			
SOW Annex-A	[SRS-7-444]	The MG SHALL provide a means to detect and reject the replay of authentication data as well as other security data and attributes.			
SOW Annex-A	[SRS-7-445]	The MG SHALL use a NPKI provided device certificate to validate its identity to other peer entities.			
SOW Annex-A	[SRS-7-446]	The MG SHALL validate the identity of other peer identities by validating the peer entities device certificate to an NPKI trust point			
SOW Annex-A	[SRS-7-447]	The MG SHALL provide measures for generating and storing audit information for security relevant events that will record access attempts to MG-protected resources by users.			
SOW Annex-A	[SRS-7-448]	The MG firmware and software SHALL be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.			
SOW Annex-A	[SRS-7-449]	The MG SHALL ensure the integrity of its update packages prior to installation.			
SOW Annex-A	[SRS-7-45]	The "ForwardEmailHL" operation SHALL be compliant with the Simple Mail Transfer Protocol (SMTP) [IETF RFC 5321, 2008].			
SOW Annex-A	[SRS-7-450]	The policy MG_IFP_CA_HL_OUT SHALL specify the actions ACTIONS_MG_CA_HL_OUT that the operation 'Enforce HL Communications IFCPE' SHALL execute for the information flow described in ([SRS-7-89]).			
SOW Annex-A	[SRS-7-451]	ACTIONS_MG_CA_HL_OUT SHALL include the following actions: • Filter traffic based on the ruleset RULESET_MG_IFCPE-CA_HL_OUT.			
SOW Annex-A	[SRS-7-452]	ACTIONS_MG_MGMT_IN SHALL include the following actions: • Filter traffic based on the ruleset RULESET_MG_IFCPE-MGT_IN.			
SOW Annex-A	[SRS-7-453]	It SHALL be possible to enable or disable the enforcement of each sub-policy in ([SRS-7-189]).			
SOW Annex-A	[SRS-7-454]	It SHALL be possible to apply each sub-policy to either information flow ('CIPE Services Low to High' and 'CIPE Services High to Low).			
SOW Annex-A	[SRS-7-455]	Cryptographic mechanisms implemented by MG_PKCS SHALL be based on Technical Implementation Guidance on Cryptographic Mechanisms in Support of Cryptographic Services [NAC AC/322-D(2012)0022, 2013].			
SOW Annex-A	[SRS-7-456]	The operation 'Configure Protection Services' MUST provide the capability to manage XML artefacts for MG_CIS.			
SOW Annex-A	[SRS-7-46]	The "ForwardEmailHL" operation SHALL be compliant with the Internet Message Format [IETF RFC 5322, 2008].			
SOW Annex-A	[SRS-7-47]	The "ForwardEmailHL" operation SHALL be compliant with the SMTP Service Extension for Secure SMTP over Transport Layer Security [IETF RFC 7817, 2016].			
SOW Annex-A	[SRS-7-48]	The "ForwardEmailHL" operation SHALL be compliant with the SMTP Service Extension for Delivery Status Notifications [IETF RFC 3461, 2003].			
SOW Annex-A	[SRS-7-49]	The "FowardEmailHL" operation SHALL be compliant with the Extensible Message Format for Delivery Status Notifications [IETF RFC 3464, 2003].			
SOW Annex-A	[SRS-7-5]	The MG SHALL offer a physical network interface MG_IF_NET_LOW that provides Ethernet connectivity to the low domain.			
SOW Annex-A	[SRS-7-50]	The 'ForwardEmailHL" operation SHALL be configurable to determine the destination host of a recipient from either DNS MX records or local configuration.			
SOW Annex-A	[SRS-7-500]	If MG_IFP_CA_HL_IN or MG_IFP_CA_HL_OUT does not permit information flow, the MG SHALL execute the actions specified in MG_IFP_CA_HL.			
SOW Annex-A	[SRS-7-501]	If MG_IFP_CA_LH_IN or MG_IFP_CA_LH_OUT do not permit information flow, the MG SHALL execute the actions specified in MG_IFP_CA_LH.			
SOW Annex-A	[SRS-7-502]	The MG management capability SHALL be installed on the management workstation.			
SOW Annex-A	[SRS-7-503]	MG_MGMT SHALL generate private keys and corresponding Certificate Signing Requests (CSRs) for signing by the appropriate NATO Registration Authority (RA).			
SOW Annex-A	[SRS-7-504]	MG_MGMT_CS SHALL update the malware/virus signatures used by the MG malware/virus scanner on a daily basis.			
SOW Annex-A	[SRS-7-505]	MG_MGMT_CM SHALL integrate the update of the virus definitions (LIST_MG_CIS_AV_MALWARE_DEFINITIONS) used by MG malware scanner with the existing capability			
SOW Annex-A	[SRS-7-506]	The MG SHALL validate a confidentiality label [STANAG 4774] against the corresponding SPIF before it is used.			
SOW Annex-A	[SRS-7-507]	MG_MGMT_CS MAY support remote checking of the status of certificates using the Online Certificate Status protocol (OCSP) [IETF RFC 6960, 2013].			
SOW Annex-A	[SRS-7-51]	The local configuration of the destination hosts for the 'ForwardEmailLH" operation SHALL allow the use of wildcards in the domain name.			
SOW Annex-A	[SRS-7-52]	The local configuration of the destination hosts for the 'ForwardEmailHL" operation SHALL allow the use of wildcards in the domain name.			
SOW Annex-A	[SRS-7-53]	The 'ForwardEmailHL" operation SHALL allow the use the best match when determining the destination host from local configuration.			
SOW Annex-A	[SRS-7-54]	The "ForwardEmailHL" operation SHALL be able to rewrite the originator and recipient email addresses in both the Simple Mail Transfer Protocol and the Internet Message Format.			
SOW Annex-A	[SRS-7-55]	The "ForwardEmailHL" address rewriting SHALL allow the rewriting of both the local-part and the domain components of the email address.			
SOW Annex-A	[SRS-7-56]	MG_DEX MUST offer a IPv4 and IPv6 [IETF RFC 791, 1981], and [IETF RFC 8200, 2017], over Ethernet interface 'Communications Access Services Management' on top of MG_IF_MGMT.			
SOW Annex-A	[SRS-7-57]	The interface 'Communications Access Services Management' MUST support an operation 'ReceiveNetworkManagement' that provides TCP/IP connectivity on the management domain by receiving IP traffic for processing by the MG.			
SOW Annex-A	[SRS-7-58]	The operation 'ReceiveNetworkManagement' MUST support error handling as specified in [IETF RFC 7414, 2015].			
SOW Annex-A	[SRS-7-59]	The interface 'Communications Access Services Management' MUST support an operation 'ForwardNetworkManagement' that forwards IP traffic to the management domain.			
SOW Annex-A	[SRS-7-6]	MG_IF_NET_LOW SHALL support an operation 'ReceiveLow' that receives (transfer-in) data from the low domain for processing by the MG.			
SOW Annex-A	[SRS-7-60]	The operation 'ForwardNetworkManagement' MUST support error handling as specified in [IETF RFC 7414, 2015].			
SOW Annex-A	[SRS-7-61]	MG_DEX MUST offer an interface 'Core Services Management' on top of 'Communications Access Services Management'.			
SOW Annex-A	[SRS-7-7]	MG_IF_NET_LOW SHALL support an operation 'ForwardLow' that forwards (transfer-out) data that has been processed by the MG to the low domain.			
SOW Annex-A	[SRS-7-70]	The interface 'Core Services Management' MUST support of the following management protocols: • Simple Network Management Protocol (SNMP) Version 3 [IETF RFC 3410 - 3418, 2002]; • Syslog; • Network Time Protocol; • Intelligent Platform Management Interface (IPMI) [IPMI V2.0, 2013]; • Hyper-Text Transport Protocol (HTTP) Web interface [IETF RFC 7230, 2014] and [IETF RFC 7231, 2014]; • Remote Desktop (RDP).			
SOW Annex-A	[SRS-7-71]	The interface 'Core Services Management' MAY support the following management protocols: • Remote Procedure Call (RPC). • Keyboard, video and mouse (KVM) over Ethernet; • Command Line interface (CLI) via Secure Shell (SSH) Transport Layer protocol [IETF RFC 4251, 2006];			
SOW Annex-A	[SRS-7-72]	The interface 'Core Services Management' MUST support an operation 'ReceiveManagementContent' that receives external management traffic for further processing.			
SOW Annex-A	[SRS-7-73]	The operation 'ReceiveManagementContent' MUST support Transport Layer Security (TLS), [IETF RFC 8446, 2018].			
SOW Annex-A	[SRS-7-74]	The operation 'ReceiveManagementContent' MUST support the Secure Shell Protocol (SSH) [IETF RFC 4251, 2006].			
SOW Annex-A	[SRS-7-75]	The operation 'ReceiveManagementContent' MUST support the invocation of the operations 'Verify' (7.6.2.2.1) and 'Decrypt' (7.6.2.2.4) at the interface 'Public Key Cryptographic Services' ([SRS-7-296]) provided by MG_PKCS ([SRS-7-294]).			
SOW Annex-A	[SRS-7-76]	The operation 'ReceiveManagementContent' SHALL pass management content in the form of a management message to the appropriate interface offered by MG_MGMT ([SRS7-302]) for further processing.			

SOW Annex-A	[SRS-7-77]	The interface 'Core Services Management' MUST support an operation 'ForwardManagementContent' that accepts outgoing management messages for further processing.			
SOW Annex-A	[SRS-7-78]	After receiving a management message from one of the interfaces offered by MG_MGMT ([SRS-7-302]), the operation 'ForwardManagementContent' SHALL forward the management message, as payload of the appropriate management protocol, to the management domain.			
SOW Annex-A	[SRS-7-79]	The operation 'ForwardManagementContent' MUST support Transport Layer Security (TLS), [IETF RFC 8446, 2018].			
SOW Annex-A	[SRS-7-8]	The MG MAY offer a physical network interface MG_IF_MGMT that provides Ethernet connectivity to the management domain.			
SOW Annex-A	[SRS-7-80]	The operation 'ForwardManagementContent' MUST support the Secure Shell Protocol (SSH) [IETF RFC 4251, 2006].			
SOW Annex-A	[SRS-7-81]	The operation 'ForwardManagementContent' MUST support the invocation of the operation 'Encrypt' (7.6.2.2.3) at the interface 'Public Key Cryptographic Services' provided by MG_PKCS ([SRS-7-294]).			
SOW Annex-A	[SRS-7-82]	The MG MUST provide an information flow control policy enforcement (IFCPE) capability MG_IFCPE that enables the MG to: • Mediate the flow of information between MG_IF_NET_HIGH and MG_IF_NET_LOW in accordance with the MG information flow policy MG_IFP; • Control incoming and outgoing management traffic at MG_IF_MGMT in accordance with the MG information flow policy MG_IFP.			
SOW Annex-A	[SRS-7-83]	Mediate the flow of information between MG_IF_NET_HIGH and MG_IF_NET_LOW in accordance with the MG information flow policy MG_IFP;			
SOW Annex-A	[SRS-7-84]	Control incoming and outgoing management traffic at MG_IF_MGMT in accordance with the MG information flow policy MG_IFP.			
SOW Annex-A	[SRS-7-86]	For the flow of information from MG_IF_NET_HIGH to MG_IF_NET_LOW, MG_IFCPE MUST offer an interface 'IFCPE Services High to Low' that accepts information for further processing.			
SOW Annex-A	[SRS-7-87]	The interface 'IFCPE Services High to Low' MUST support an operation 'Enforce HL Communications IFCPE' that enforces the policy MG_IFP_CA_HL.			
SOW Annex-A	[SRS-7-88]	The operation 'Enforce HL Communications IFCPE' SHOULD enforce the policy MG_IFP_CA_HL_IN on the following information flow: • Source: Communications Access Services HL Interface -> ReceiveInternalNetworkHL; • Destination: Business Support Services HL Interface -> ReceiveEmailHL; • Information: SMTP(S) traffic; • Operation: pass SMTP(S) traffic by ensuring the following conditions: o MG_IFP_CA_HL_IN permits information flow.			
SOW Annex-A	[SRS-7-89]	The operation 'Enforce HL Communications IFCPE' SHALL enforce the policy MG_IFP_CA_HL_OUT on the following information flow: • Source: SOA Platform HL Interface -> ForwardEmailHL; • Destination: Communications Access Services HL Interface -> ForwardNetworkHL; • Information: SMTP(S) traffic; • Operation: pass SMTP(S) traffic by ensuring the following conditions: o MG_IFP_CA_HL_OUT permits information flow.			
SOW Annex-A	[SRS-7-9]	If the MG does not offer a physical network interface MG_IF_MGMT, the MG SHALL offer a logical network interface MG_IF_MGMT on top of MG_IF_NET_HIGH.			
SOW Annex-A	[SRS-7-90]	For every action taken, the operation 'Enforce HL Communications IFCPE' SHALL invoke the operation 'Log' at the interface 'Event Management' and log the action.			
SOW Annex-A	[SRS-7-91]	If MG_IFP_CA_HL does not permit the release of information due to a policy violation, the MG SHALL invoke the operation 'Log' at the interface 'Event Management' and log the outcome O_MG_IFCPE.			
SOW Annex-A	[SRS-7-92]	The MG SHALL ensure that no illicit information flows exist to circumvent the enforcement of MG_IFP_CA_HL			
SOW Annex-A	[SRS-7-93]	The interface 'IFCPE Services High to Low' MUST support an operation 'Enforce HL Business Support IFCPE' that enforces the policy IEG-C_IFP_BS_EMAIL_HL.			
SOW Annex-A	[SRS-7-94]	The operation 'Enforce HL Business Support IFCPE' SHALL enforce the policy IEG-C_IFP_BS_EMAIL_HL on the following information flow: • Source: Business Support Services HL Interface->ReceiveEmailHL; • Destination: Business Support Services HL Interface >ForwardEmailHL; • Information: SMTP Messages; • Operation: pass SMTP Messages from source to destination ensuring the following conditions: o the SMTP Message has been processed by the MG content inspection policy enforcement capability MG_CIPE ([SRS-7-169]) based on the content inspection policy MG_CIP_HL (Table 19, 7.5.4.3 and 7.5.4.4); o Based on the outcome of processing by MG_CIPE, IEG-C_IFP_BS_EMAIL_HL permits the release of the SMTP Message to the low domain.			
SOW Annex-A	[SRS-7-95]	The operation 'Enforce HL Business Support IFCPE' MUST support the invocation of the operation 'Enforce HL Business Support CIPE' at the interface 'CIPE Services High to Low' ([SRS-7-173]). The operation 'Enforce HL Business Support CIPE' SHALL take as input: • The SMTP message that is being processed; • The policy MG_CIP_HL.			
SOW Annex-A	[SRS-7-96]	If IEG-C_IFP_BS_EMAIL_HL does not permit the release of information, the MG SHALL execute the actions specified in IEG-C_IFP_BS_EMAIL_HL.			
SOW Annex-A	[SRS-7-97]	For every action taken, the operation 'Enforce HL Business Support IFCPE' SHALL invoke the operation 'Log' (7.7.7.1.1) at the interface 'Event Management' ([SRS-7-392]) and log the action.			
SOW Annex-A	[SRS-7-98]	If IEG-C_IFP_BS_EMAIL_HL does not permit the release of information due to a policy violation, the MG SHALL invoke the operation 'Log' 7.7.7.1.1) at the interface 'Event Management' ([SRS-7-392]) and log the outcome O_MG_IFCPE ([SRS-7-91]).			
SOW Annex-A	[SRS-7-99]	The MG SHALL ensure that no illicit information flows exist to circumvent the enforcement of IEG-C_IFP_BS_EMAIL_HL.			
SOW Annex-A	[SRS-8-1]	The IEG-C SHALL be located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the IEG-C.			
SOW Annex-A	[SRS-8-10]	The TBP SHALL provide mechanisms that control a user's logical access to the TOE and to explicitly deny access to specific users when appropriate.			
SOW Annex-A	[SRS-8-11]	The IEG-C SHALL be able to recognize and discard invalid or malicious input provided by users.			
SOW Annex-A	[SRS-8-12]	The IEG-C SHALL be capable of maintaining protection policy enforcement if it is unable to communicate with the Policy Enforcement module which provided it the policy.			
SOW Annex-A	[SRS-8-13]	The IEG-C SHALL provide a mechanism to identify and rectify contradictory policy data.			
SOW Annex-A	[SRS-8-14]	The IEG-C SHALL enable enforcement of information flow between the IEG-C components.			
SOW Annex-A	[SRS-8-15]	The IEG-C SHALL enable enforcement of content inspection between the IEG-C components.			
SOW Annex-A	[SRS-8-16]	The IEG-C SHALL validate the origin, integrity and binding [STANAG 4778 of a security label [STANAG 4774] to a data object before it is used.			
SOW Annex-A	[SRS-8-17]	The Data Protection Module SHALL provide a NATO approved cryptographic sub-component with NATO-approved methods for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys), and for cryptographic operations (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services) as described in [NAC AC/322-D(2007)0002-REV1, 2015].			
SOW Annex-A	[SRS-8-18]	The Data Protection Module cryptographic sub-component is validated according validated to at least FIPS 140-2 Level 2 [FIPS 140-2, 2001], or otherwise verified to an equivalent level of functionality and assurance by a NATO nation COMSEC authority. Ref: [NAC AC/322-D(2004)0024-REV3-COR1, 2018]			
SOW Annex-A	[SRS-8-19]	The Data Protection Module SHALL provide capability to protect against network-based reconnaissance (probing for information about a monitored network or its endpoints), such as through use of various scanning or mapping techniques. Ref: [NC3B AC/322-D(2004)0019 (INV), 2004]			
SOW Annex-A	[SRS-8-2]	Utilisation of modern IA techniques and compliancy with the cyber-defence services SHALL be followed.			
SOW Annex-A	[SRS-8-2]	The Infrastructure Platform SHALL provide a NATO approved malware scanning capability [NC3B AC/322-D(2004)0019 (INV), 2004].			
SOW Annex-A	[SRS-8-20]	The Data Protection Module SHALL provide capability to protect against attacks that are targeted at obstructing the normal function of monitored networks, endpoints, or services, such as through denial of service attacks. Ref: [NC3B AC/322-D(2004)0019 (INV), 2004]			
SOW Annex-A	[SRS-8-21]	The Data Protection Module SHALL provide capability to protect against disclosing or transmitting information in violation of the policy.			
SOW Annex-A	[SRS-8-22]	The IEG-C SHALL apply analytical processes to network traffic data collected from monitored networks and derive conclusions about potential intrusions or network traffic policy violations.			
SOW Annex-A	[SRS-8-23]	The IEG-C shall provide mechanisms that mitigate attempts to exhaust resources provided by the TOE (e.g., resulting in denying access to high network resources).			
SOW Annex-A	[SRS-8-24]	The Data Protection Module SHALL provide capability to protect against gaining inappropriate access to one or more networks, endpoints, or services, such as through transmitting malicious executable code, scripts, or commands. Ref: [NC3B AC/322-D(2004)0019 (INV), 2004]			
SOW Annex-A	[SRS-8-25]	The IEG-C SHALL ensure that is protection policy information is transmitted to the Policy Enforcement Module in a secure and timely manner so that there is assurance that the correct policy is being enforced.			
SOW Annex-A	[SRS-8-26]	The IEG-C SHALL ensure that communications between distributed components of the TOE are not subject to unauthorized modification or disclosure.			
SOW Annex-A	[SRS-8-27]	The IEG-C SHALL provide a means to ensure that administrators are not communicating with some other entity pretending to be the TOE when supplying identification and authentication data.			
SOW Annex-A	[SRS-8-28]	The IEG-C SHALL provide a mechanism to securely validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF.			
SOW Annex-A	[SRS-8-29]	The IEG-C SHALL contain the ability to validate the identity of other TOE components prior to distributing data to them.			

SOW Annex-A	[SRS-8-3]	The IEG-C SHALL consider and apply the following directions, guidance and obligation within the INFOSEC technical and implementation directive for the interconnection of networks: • AC/322-D(2004)0024-REV3-COR1 "CIS Security Technical and Implementation Directive on the NATO PKI Certificate Policy" • AC/35-D/1021-REV3, dated 31 Jan 2012 "Guidelines for the security accreditation of communication and information systems (CIS)" • AC/35 D/2004 Rev3 15 Nov 2013 "Primary Directive on CIS Security" • AC/322-D/0047-REV2 (INV) 11 March 2009 "INFOSEC Technical & Implementation Directive on cryptographic security and cryptographic mechanisms"			
SOW Annex-A	[SRS-8-3]	The Infrastructure Platform SHALL provide capability to ensure that only authorized communications are allowed between the high and low networks.			
SOW Annex-A	[SRS-8-30]	The IEG-C SHALL provide a means to detect and reject the replay of authentication data as well as other TSF data and security attributes.			
SOW Annex-A	[SRS-8-31]	The IEG-C SHALL provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users.			
SOW Annex-A	[SRS-8-32]	The IEG-C shall provide the capability to protect audit information.			
SOW Annex-A	[SRS-8-33]	The IEG-C SHALL provide the capability to selectively view audit information, and alert the administrator of identified potential security violations.			
SOW Annex-A	[SRS-8-34]	The IEG-C SHALL provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.			
SOW Annex-A	[SRS-8-35]	An IEG-C SHALL ensure that information exists that allows administrators to discover unintentional issues with the configuration and operation of the operating system and discover its cause. Gathering event information and immediately transmitting it to another system can also enable incident response in the event of system compromise.			
SOW Annex-A	[SRS-8-36]	The IEG-C SHALL provide an administrator role to isolate administrative actions, and to make the administrative functions available locally and remotely.			
SOW Annex-A	[SRS-8-37]	The IEG-C SHALL provide all the functions and facilities necessary to support the administrators in their management of the security of the IEG-C, and restrict these functions and facilities from unauthorized use.			
SOW Annex-A	[SRS-8-38]	The IEG-C SHALL display an advisory warning regarding use of the IEG-C.			
SOW Annex-A	[SRS-8-39]	The configuration of, and all changes to, the IEG-C and its development evidence SHALL be analysed, tracked, and controlled throughout the IEG-C's development.			
SOW Annex-A	[SRS-8-4]	The Infrastructure Platform SHALL provide reliable time data to the IEG-C.			
SOW Annex-A	[SRS-8-40]	The IEG-C SHALL provide a mode from which recovery or initial start-up procedures can be performed.			
SOW Annex-A	[SRS-8-41]	The IEG-C SHALL collect and store information about all events that may indicate a policy violation related to misuse, inappropriate access, or malicious activity on monitored networks.			
SOW Annex-A	[SRS-8-42]	The Infrastructure Platform firmware and software SHALL be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.			
SOW Annex-A	[SRS-8-50]	The IEG-C firmware and software SHALL be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.			
SOW Annex-A	[SRS-8-43]	The IEG-C SHALL ensure the integrity of their update packages. OSs are seldom if ever shipped without errors, and the ability to deploy patches and updates with integrity is critical to enterprise network security. Conformant IEG-Cs provide execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems.			
SOW Annex-A	[SRS-8-44]	The IEG-C SHALL provide a capability to test the TSF to ensure the correct operation of the TSF in its operational environment.			
SOW Annex-A	[SRS-8-45]	The IEG-C SHALL undergo appropriate independent vulnerability analysis and penetration testing to demonstrate the design and implementation of the TOE does not allow attackers with medium attack potential to violate the TOE's security policies.			
SOW Annex-A	[SRS-8-46]	The IEG-C SHALL undergo appropriate security functional testing that demonstrates the TSF satisfies the security functional requirements.			
SOW Annex-A	[SRS-8-47]	The IEG-C SHALL respond appropriately to its analytical conclusions about policy violations.			
SOW Annex-A	[SRS-8-48]	The IEG-C SHALL ensure that any information contained in a protected resource is not released when the resource is reallocated; this includes that no residual information from a previously relayed message is transmitted.			
SOW Annex-A	[SRS-8-49]	The TSF SHALL maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure.			
SOW Annex-A	[SRS-8-5]	The IEG-C is a distributed system, therefore, the TBP SHALL implement measures to protect against eavesdropping between components of the IEG-C that are distributed.			
SOW Annex-A	[SRS-8-6]	The TBP consists of hardware (processors, memory, and devices), firmware and the operating system(s). The TBP SHALL be configured according to relevant NATO guidance and directives [NAC AC/322-D/0048-REV3, 2019]			
SOW Annex-A	[SRS-8-7]	The TBP SHALL protect components and areas of main memory from being directly accessed (without that access being mediated by the operating system) by untrusted subjects.			
SOW Annex-A	[SRS-8-8]	The TBP SHALL protect any other function of the underlying platform from being used by untrusted subjects in a way that would violate the security policy of the operating system.			
SOW Annex-A	[SRS-8-9]	The TBP SHALL provide reliable time data to all components of the IEG-C.			
SOW Annex-A	[SRS-9-1]	All Management capabilities MUST provide support for multiple concurrent administrators with access control to enable simultaneous access to the management capability from potentially distributed consoles with appropriately administered levels of access.			
SOW Annex-A	[SRS-9-10]	Remote Management traffic MUST be encrypted.			
SOW Annex-A	[SRS-9-100]	The IEG-C 'Cyber Defence' Interface SHALL pass outgoing 'Assess' Cyber Defence Messages to the interface 'Core Services Management' for further processing.			
SOW Annex-A	[SRS-9-101]	The IEG-C SHALL provide the Cyber Defence administrator with the required functionality to take the required action to dynamically mitigate the risk identified by a suspected attack/fault.			
SOW Annex-A	[SRS-9-102]	The IEG-C SHALL provide the capability to control traffic flows including termination, throttling to a certain level of bandwidth or with a certain delay, redirection, or otherwise modify the flow for the purpose of stopping or mitigating an attack or fault.			
SOW Annex-A	[SRS-9-103]	The IEG-C SHALL provide capability for traffic flows to be terminated or limited in capacity in order to stop or reduce the effect of an attack or a fault.			
SOW Annex-A	[SRS-9-105]	The operation 'Respond' SHALL support Cyber Defence Messages of the following types: • Secure Shell (SSH, [IETF RFC 4253, 2006]); • Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]); • HTTP over TLS ([IETF RFC 2818, 2000]).			
SOW Annex-A	[SRS-9-106]	The IEG-C 'Cyber Defence' Interface SHALL pass outgoing 'Respond' Cyber Defence Messages to the interface 'Core Services Management' for further processing.			
SOW Annex-A	[SRS-9-107]	The IEG-C SHALL provide the Cyber Defence administrator with the required functionality to take the required action to recover from an attack/fault.			
SOW Annex-A	[SRS-9-108]	The IEG-C SHALL provide the capability to restore IEG-C components that were affected by an attack/fault.			
SOW Annex-A	[SRS-9-109]	The operation 'Recover' SHALL support Cyber Defence Messages of the following types: • Secure Shell (SSH, [IETF RFC 4253, 2006]); • Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]); • HTTP over TLS ([IETF RFC 2818, 2000]).			
SOW Annex-A	[SRS-9-11]	The IEG-C Management Interface MUST support Transport Layer Security (TLS, [IETF RFC 8446, 2018]).			
SOW Annex-A	[SRS-9-110]	The IEG-C 'Cyber Defence' Interface SHALL pass outgoing 'Recover' Cyber Defence Messages to the interface 'Core Services Management' for further processing.			
SOW Annex-A	[SRS-9-111]	The IEG-C SHALL provide the capability to allow the Audit Administrator to fulfil their role.			
SOW Annex-A	[SRS-9-112]	The IEG-C SHALL be interoperable with NATO auditing and system management tools.			
SOW Annex-A	[SRS-9-113]	The IEG-C SHALL provide the capability to detect and create records of security-relevant events associated with users.			
SOW Annex-A	[SRS-9-114]	The IEG-C SHALL provide the capability to detect and create records of security-relevant events associated with end users requests for accessing information cross domain.			
SOW Annex-A	[SRS-9-115]	The IEG-C SHALL provide the capability to appropriately classify and protect audit information in accordance with NATO security policy.			
SOW Annex-A	[SRS-9-116]	The IEG-C SHALL include mechanisms to protect audit logs from unauthorised access, modification and deletion.			
SOW Annex-A	[SRS-9-117]	The IEG-C SHALL provide the capability to selectively view audit information, and alert the Audit Administrator of identified potential security violations.			
SOW Annex-A	[SRS-9-118]	The IEG-C SHALL provide reliable time stamps and the capability for the Audit Administrator to set the time used for these time stamps.			
SOW Annex-A	[SRS-9-119]	The IEG-C SHALL generate and maintain an audit log for each of the general auditable events: • IEG-C start-up and shutdown • IEG-C Users logon and logoff • Creation, modification (i.e. changes to permissions) or deletion of user accounts • Changes to security related system management functions • Audit log access • Creation, modification or deletion of audit log records • Invocation of privileged operations • Modification to IEG-C access rights • Unauthorised attempts to access IEG-C system files			
SOW Annex-A	[SRS-9-12]	The IEG-C Management Interface MUST support Datagram Transport Layer Security (DTLS, [IETF RFC 6353, 2011]).			

SOW Annex-A	[SRS-9-120]	The IEG-C SHALL generate and maintain an audit log for each of the Data Exchange Services auditable events: • Data Exchange Services Start-up and shutdown • Unauthorised attempts to request access to information cross domain • Unauthorised attempts to modify Data Exchange Services configuration • Failed Data Exchange Services operations			
SOW Annex-A	[SRS-9-121]	The IEG-C SHALL generate and maintain an audit log for each of the Protection Services auditable events: • Protection Services start-up and shutdown • Failed Protection Services operations • Unauthorised attempts to modify Protection Services configuration • Creation, modification and deletion of Public Key Cryptographic Services keying material • Updates of Intrusion Detection Services IDS signatures • Updates of Content Inspection Services content filters • Failed certificate path validation and revocation			
SOW Annex-A	[SRS-9-122]	The IEG-C SHALL generate and maintain an audit log for each of the Protection Policy Enforcement Services auditable events: • Protection Policy Enforcement Services start-up and shutdown • Failed Protection Policy Enforcement Services operations • Unauthorised attempts to create, modify or delete Information Flow Control policies • Unauthorised attempts to create, modify or delete Content Inspection policies			
SOW Annex-A	[SRS-9-123]	The IEG-C SHALL archive the audit log after a period of time as configured by the Audit Administrator.			
SOW Annex-A	[SRS-9-124]	By default the audit log SHALL be archived daily.			
SOW Annex-A	[SRS-9-125]	The IEG-C SHALL automatically back up audit logs at configurable intervals.			
SOW Annex-A	[SRS-9-126]	The IEG-C SHALL provide integrity checking countermeasures to ensure that the audit log has been archived correctly.			
SOW Annex-A	[SRS-9-127]	The IEG-C SHALL alert the Audit Administrator when the audit log exceeds a configurable percentage of the configurable maximum permitted size.			
SOW Annex-A	[SRS-9-128]	By default the configurable percentage SHALL be 90% of the configurable maximum permitted size.			
SOW Annex-A	[SRS-9-13]	The IEG-C MUST offer the 'Communications Access Management' Interface on top of the IEG-C Management interface.			
SOW Annex-A	[SRS-9-14]	The IEG-C MUST offer the 'Core Services Management' Interface on top of the 'Communications Access Management' Interface			
SOW Annex-A	[SRS-9-15]	The IEG-C MUST support the 'ReceiveManagementContent' operation to provide connectivity for administrators on the MANAGEMENT DOMAIN.			
SOW Annex-A	[SRS-9-16]	The operation 'ReceiveManagementContent' SHALL pass management content to the appropriate interface (see Sections 9.2, [SRS-9-83] and [SRS-9-98]).			
SOW Annex-A	[SRS-9-17]	The IEG-C MUST support the 'ForwardManagementContent' operation that forwards management traffic to the MANAGEMENT DOMAIN.			
SOW Annex-A	[SRS-9-18]	After receiving management content from the appropriate interface (see Sections 9.2, [SRS-9-83] and [SRS-9-98].), the operation 'ForwardManagementContent' SHALL forward the management content to the MANAGEMENT DOMAIN.			
SOW Annex-A	[SRS-9-19]	An Enterprise CMDB already exists, and SHALL be used as the underpinning of the Platform's configuration management as well.			
SOW Annex-A	[SRS-9-2]	Figure 32 illustrates the interfaces that MUST be provided by the IEG-C for managing the IEG-C remotely and locally.			
SOW Annex-A	[SRS-9-20]	The IEG-C SHALL support the Enterprise Configuration Management via an interface with the Enterprise configuration management database (BMC ITSM Atrium CMDB) to track IEG-C assets and their configuration information.			
SOW Annex-A	[SRS-9-200]	The patching of IEG-C components SHAL be performed centrally from the Service Operation Centre (SOC).			
SOW Annex-A	[SRS-9-201]	For all its components the IEG-C SHALL support the generation of cybersecurity-related log, alert, and event data in accordance with the NATO Enterprise Security Monitoring Guidance [NCI Agency TR/2017/NCB010400/12, 2017] and the Technical and Implementation Directive on CIS Security [NAC AC/322-D/0048-REV3, 2019].			
SOW Annex-A	[SRS-9-202]	For all its components the IEG-C SHALL support the ingestion of cybersecurity-related log, alert, and event data in the SIEM solution that is operated by NCSC.			
SOW Annex-A	[SRS-9-203]	For all its components the IEG-C SHALL ensure that all cybersecurity-related log, alert, and event data can be parsed correctly by the SIEM solution that is operated by NCSC.			
SOW Annex-A	[SRS-9-204]	All audit logs SHALL record the date, time, details of change and the user.			
SOW Annex-A	[SRS-9-21]	The IEG-C MUST offer an interface 'SMC Configuration Management' that accepts an incoming 'SMC Message' for further processing.			
SOW Annex-A	[SRS-9-22]	The 'SMC Configuration Management' Interface MUST provide the capability to manage the underlying operating system(s) hosting all the services provided by the IEG-C.			
SOW Annex-A	[SRS-9-23]	The 'SMC Configuration Management' Interface MUST provide the capability to configure, deploy and decommission Data Exchange Services depending upon the information exchange requirement(s) that is (are) being supported.			
SOW Annex-A	[SRS-9-24]	The 'SMC Configuration Management' Interface MUST provide the capability to configure, deploy and decommission Protection Services depending upon the information exchange requirement(s) that is (are) being supported.			
SOW Annex-A	[SRS-9-25]	The 'SMC Configuration Management' Interface MUST provide the capability to provides the ability to change, capture, duplicate, backup or restore the configuration of the Protection Policy Enforcement Services depending upon the information exchange requirement(s) that is (are) being supported.			
SOW Annex-A	[SRS-9-26]	The 'SMC Configuration Management' Interface MUST support the following operations: • 'Configure OS'; • 'Configure Data Exchange Services'; • 'Configure Protection Services'; and, • 'Configure Protection Policy Enforcement Services'.			
SOW Annex-A	[SRS-9-27]	The operation 'Configure OS' SHALL support SMC Messages of the following types: • Secure Shell (SSH, [IETF RFC 4253, 2006]); • Network Time Protocol (NTP, [IETF RFC 5905, 2010]); • Remote Desktop Protocol (RDP); • Intelligent Platform Management Interface (IPMI, [IPMI V2.0, 2013]); • Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]).			
SOW Annex-A	[SRS-9-28]	The operation 'Configure OS' SHALL support the management of the IEG-C hardware (virtual or physical) and software resources including configuration of common services provided by the operating system (OS) for applications running on the operating system. These common services include application execution, input/output operations, file system, communication, resource allocation, control access to OS resources and time synchronisation.			
SOW Annex-A	[SRS-9-29]	The operation 'Configure Data Exchange Services' SHALL support SMC Messages of the following types: • Secure Shell (SSH, [IETF RFC 4253, 2006]); • Remote Desktop Protocol (RDP); • Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]).			
SOW Annex-A	[SRS-9-3]	The IEG-C MUST provide the capability to be managed remotely from a central location on the HIGH DOMAIN.			
SOW Annex-A	[SRS-9-30]	The operation 'Configure Protection Services' SHALL support SMC Messages of the following types: • Secure Shell (SSH, [IETF RFC 4253, 2006]); • Remote Desktop Protocol (RDP); • Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]).			
SOW Annex-A	[SRS-9-31]	The operation 'Configure Protection Policy Enforcement Services' SHALL support SMC Messages of the following types: • Secure Shell (SSH, [IETF RFC 4253, 2006]); • Remote Desktop Protocol (RDP); • Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]).			
SOW Annex-A	[SRS-9-32]	The IEG-C 'SMC Configuration Management' Interface SHALL pass outgoing SMC Messages to the interface 'Core Services Management' for further processing.			
SOW Annex-A	[SRS-9-34]	The IEG-C SHALL collect events generated from all IEG-C services and forward them to the Enterprise Event Management System.			
SOW Annex-A	[SRS-9-35]	The IEG-C SHOULD support monitoring based on the Microsoft System Center Operations Manager (SCOM).			
SOW Annex-A	[SRS-9-36]	The IEG-C SHALL support SNMP v3 [IETF RFC 3412, 2002] with standards-based and proprietary-specific Management Information Bases (MIBs).			
SOW Annex-A	[SRS-9-37]	The IEG-C SHALL provide a toolset which allows Administrators to define, filter, correlate and group events according to their context, criticality, source and impacts.			
SOW Annex-A	[SRS-9-38]	The IEG-C SHALL provide an event correlation toolset that can be either customizable or adaptive to detect normal and abnormal behaviour patterns.			
SOW Annex-A	[SRS-9-39]	The IEG-C MUST offer an interface 'SMC Event Management' that accepts an incoming 'SMC Message' for further processing.			
SOW Annex-A	[SRS-9-4]	To support remote management from a central location the IEG-C MUST offer the physical (or logical) IEG-C Management Interface implemented on top of the IEG-C High Domain Interface as described in Section 3.2.			
SOW Annex-A	[SRS-9-40]	The 'SMC Event Management' Interface MUST support the following operations:			
SOW Annex-A	[SRS-9-41]	The IEG-C SHALL support Data Exchange Services logging for monitoring access requests for information from both the High Domain and the Low Domain.			
SOW Annex-A	[SRS-9-42]	The IEG-C SHALL provide the capability to examine recorded historical logs and archives.			
SOW Annex-A	[SRS-9-43]	The IEG-C SHALL support the correlation of requests and responses in order to track all responses (or faults) with the correct request for information access.			
SOW Annex-A	[SRS-9-44]	The IEG-C SHALL log request and response attributes to include:			
SOW Annex-A	[SRS-9-45]	The IEG-C SHALL also provide functionality to log attributes extracted from the payload.			
SOW Annex-A	[SRS-9-46]	The IEG-C SHALL provide functionality to log selectively whole messages based on pre-configured criteria or filter (e.g. policy based).			
SOW Annex-A	[SRS-9-47]	The IEG-C SHALL provide a log analysis tool that allows a search for log events based on combinations of search criteria across all fields in the log record format supported by this system.			

SOW Annex-A	[SRS-9-49]	The IEG-C SHALL provide the capability to aggregate generated log messages for all instances of services of IEG-C.			
SOW Annex-A	[SRS-9-5]	The IEG-C MUST provide the capability to be managed locally.			
SOW Annex-A	[SRS-9-50]	The operation 'Log' SHALL support SMC Messages of the following types: • Syslog Message [IETF RFC 5424, 2009]; and, • Hypertext Transport Protocol Message (HTTP/1.1, [IETF RFC 7230, 2014], HTPP/2.0 [IETF RFC 7540, 2015]).			
SOW Annex-A	[SRS-9-51]	The IEG-C 'SMC Event Management' Interface SHALL pass outgoing 'Log' SMC Messages to the interface 'Core Services Management' for further processing.			
SOW Annex-A	[SRS-9-52]	The IEG-C SHALL provide a toolset to configure rule based event filtering, and to automate alert triggering capabilities.			
SOW Annex-A	[SRS-9-53]	The IEG-C SHALL provide functionality to generate alerts associated with IEG-C services to include: • breach of performance or capacity thresholds; • SLAs can't be met; and • specific mechanisms to enforce SLAs were activated (e.g. throttling).			
SOW Annex-A	[SRS-9-54]	The IEG-C SHALL provide functionality to generate an alert about stalled processes (e.g. a compromised content filter).			
SOW Annex-A	[SRS-9-55]	The operation 'Alert' SHALL support SMC Messages of the following types: • Simple Network Management Protocol (SNMP) v3 Message [IETF RFC 3410-3418, 2002] • Syslog [IETF RFC 5424, 2009];			
SOW Annex-A	[SRS-9-56]	The IEG-C 'SMC Event Management' Interface SHALL pass outgoing 'Alert' SMC Messages to the interface 'Core Services Management' for further processing.			
SOW Annex-A	[SRS-9-57]	The IEG-C SHALL provide operational and historical reports on events.			
SOW Annex-A	[SRS-9-58]	The IEG-C SHALL provide a toolset allowing for custom report building and saving.			
SOW Annex-A	[SRS-9-59]	The IEG-C SHALL be able to generate • SLA compliance reports • error/exception reports • service usage reports • other customizable reports based on captured metrics which can be filtered and sorted based on various criteria			
SOW Annex-A	[SRS-9-6]	To support local management the IEG-C MUST offer a physical network interface providing Ethernet connectivity to the management users on a separate security domain depicted as the MANAGEMENT DOMAIN in Figure 32			
SOW Annex-A	[SRS-9-60]	The IEG-C SHALL be able to provide performance trend analysis.			
SOW Annex-A	[SRS-9-61]	The operation 'Report' SHALL support SMC Messages of the following types: • Simple Network Management Protocol (SNMP) v3 Message [IETF RFC 3410-3418, 2002] • Comma Separated Values (CSV)			
SOW Annex-A	[SRS-9-62]	The IEG-C 'SMC Event Management' Interface SHALL pass outgoing 'Report' SMC Messages to the interface 'Core Services Management' for further processing.			
SOW Annex-A	[SRS-9-63]	The IEG-C MUST offer an interface 'SMC Performance Management' that accepts an incoming 'SMC Message' for further processing.			
SOW Annex-A	[SRS-9-64]	The 'SMC Performance Management' Interface MUST support the following operations: • Monitor'; and • 'Meter';			
SOW Annex-A	[SRS-9-65]	The IEG-C SHALL monitor the status and quality of service, (including availability, performance, and utilisation) of the IEG-C infrastructure and the IEG-C Services hosted on the IEG-C.			
SOW Annex-A	[SRS-9-66]	The IEG-C SHALL provide functionality for real time monitoring of IEG-C Services against expected KPI, SLA, or other metric thresholds as configured.			
SOW Annex-A	[SRS-9-67]	The IEG-C SHALL provide visibility on usage patterns over daily, monthly and variable periods. This toolset shall support trend and abnormal behaviour analysis.			
SOW Annex-A	[SRS-9-68]	The IEG-C SHALL provide customizable dashboards for monitoring selected statistics and metrics for IEG-C services.			
SOW Annex-A	[SRS-9-69]	The IEG-C SHALL provide the capability to monitor requests for information access attempts cross domain through the IEG-C services.			
SOW Annex-A	[SRS-9-7]	The IEG-C Management Interface MUST support the operation 'ReceiveNetworkManagement' as specified in [NCIA TR/2016/NSE010871/01, 2017] section A.2.2.3.			
SOW Annex-A	[SRS-9-70]	The IEG-C SHALL provide functionality to monitor service faults and exceptions.			
SOW Annex-A	[SRS-9-71]	The operation 'Monitor' SHALL support SMC Messages of the following types: • Simple Network Management Protocol (SNMP) v3 Message [IETF RFC 3410-3418, 2002]			
SOW Annex-A	[SRS-9-72]	The IEG-C 'SMC Performance Management' Interface SHALL pass outgoing 'Monitor' SMC Messages to the interface 'Core Services Management' for further processing.			
SOW Annex-A	[SRS-9-73]	The IEG-C SHALL be able to collect and present the statistics on service utilisation broken down by end user or system which can be used for metering, billing and other purposes.			
SOW Annex-A	[SRS-9-74]	The IEG-C SHALL aggregate collected statistics for a given end user or system or group of end user or system over specified periods of time.			
SOW Annex-A	[SRS-9-75]	The IEG-C SHALL archive and make available for retrieval and reporting collected and aggregated statistics.			
SOW Annex-A	[SRS-9-76]	The operation 'Meter' SHALL support SMC Messages of the following types: • Simple Network Management Protocol (SNMP) v3 Message [IETF RFC 3410-3418, 2002]			
SOW Annex-A	[SRS-9-77]	The IEG-C 'SMC Performance Management' Interface SHALL pass outgoing 'Meter' SMC Messages to the interface 'Core Services Management' for further processing.			
SOW Annex-A	[SRS-9-78]	The IEG-C SHALL provide the capability to allow the CIS Security Administrator to fulfil their role.			
SOW Annex-A	[SRS-9-79]	The IEG-C MUST offer an interface 'CIS Security' that accepts an incoming 'CIS Security Message' for further processing.			
SOW Annex-A	[SRS-9-8]	The IEG-C Management Interface MUST support the operation 'ForwardNetworkManagement' as specified in [NCIA TR/2016/NSE010871/01, 2017] section A.2.2.3.			
SOW Annex-A	[SRS-9-80]	The 'Cyber Defence' Interface MUST support the following operations: • 'Manage Public Key Material'; • 'Manage Protection Policies'; and, • 'Review'.			
SOW Annex-A	[SRS-9-81]	The IEG-C SHALL provide the Security administrator the ability to perform all necessary functions regarding the management of cryptographic key material.			
SOW Annex-A	[SRS-9-82]	The management of key material SHALL be compliant with CIS Security Technical and Implementation Guidance in Support of Public Key Infrastructure - Cryptographic Aspects [NAC AC/322-D(2007)0002-REV1, 2015].			
SOW Annex-A	[SRS-9-84]	The IEG-C 'CIS Security' Interface SHALL pass outgoing 'Manage Public Key Material' CIS Security Messages to the interface 'Core Services Management' for further processing.			
SOW Annex-A	[SRS-9-85]	The IEG-C SHALL provide the capability for a Security administrator to manage the full lifecycle of the Information Flow Control Policies and the Content Inspection Policies that are required to be enforced by the Protection Policy Enforcement Services dependent upon the information exchange requirements.			
SOW Annex-A	[SRS-9-86]	The IEG-C SHALL provide the capability to support the creation, modification and deletion of the protection policies including the activation and de-activation of those protection policies.			
SOW Annex-A	[SRS-9-87]	The IEG-C 'Manage Protection Policies' operation SHALL also support backing up and restoring of policies.			
SOW Annex-A	[SRS-9-88]	The IEG-C SHALL provide the Security administrator with the capability to manage the Protection Services with tasks such as update IDS signatures, anti-virus signatures, manage content filters and patch hardware and software.			
SOW Annex-A	[SRS-9-89]	The operation 'Manage Protection Policies' SHALL support CIS Security Messages of the following types:			
SOW Annex-A	[SRS-9-9]	The IEG-C Management Interface SHALL be managed using one or more of the following protocols: • HyperText Transport Protocol (HTTP) [IETF RFC 7230, 2014]; • Secure Shell Protocol (SSH) [IETF RFC 4251, 2006]; • Remote Desktop Protocol; • Keyboard, Video and Mouse (KVM) over Ethernet; • Simple Network Management Protocol (SNMP) v3 [IETF RFC 3410 – 3418, 2002].			
SOW Annex-A	[SRS-9-90]	The IEG-C 'CIS Security' Interface SHALL pass outgoing 'Manage Protection Policies' CIS Security Messages to the interface 'Core Services Management' for further processing.			
SOW Annex-A	[SRS-9-91]	The IEG-C SHALL provide the capability to the Audit manager to review audit logs.			
SOW Annex-A	[SRS-9-92]	The operation 'Review' SHALL support CIS Security Messages of the following types: • Secure Shell (SSH, [IETF RFC 4253, 2006]); • Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]); • HTTP over TLS ([IETF RFC 2818, 2000]).			
SOW Annex-A	[SRS-9-93]	The IEG-C SHALL provide the capability to allow the Cyber Defence Administrator to fulfil their role.			
SOW Annex-A	[SRS-9-94]	The IEG-C MUST offer an interface 'Cyber Defence' that accepts an incoming 'Cyber Defence Message' for further processing.			
SOW Annex-A	[SRS-9-95]	The 'Cyber Defence' Interface MUST support the following operations: • 'Assess'; • 'Respond'; and, • 'Recover'.			
SOW Annex-A	[SRS-9-96]	The IEG-C SHALL provide the Cyber Defence administrator with the capability to assess damage and attacks/faults identifying IEG-C components that have been affected by attacks and faults.			
SOW Annex-A	[SRS-9-97]	The IEG-C SHALL support analysis and evaluation of attacks.			
SOW Annex-A	[SRS-9-98]	For all its components the IEG-C SHALL support the aggregation of cybersecurity-related log, alert, and event data to a central repository or log aggregator as provided by the monitoring infrastructure in use by NCSC..			

SOW Annex-A	[SRS-9-99]	The operation 'Assess' SHALL support Cyber Defence Messages of the following types: • Secure Shell (SSH, [IETF RFC 4253, 2006]); • Hypertext Transport Protocol Message (HTTP, [IETF RFC 7230, 2014]); • HTTP over TLS ([IETF RFC 2818, 2000]).			

Provided/Detailed
Partial
Deviation proposed
Not Detailed

BI
SOW
SRS