40.3.6.1 the fabricated parts, work in process, completed work, Work, and other material produced as a part of, or acquired in connection with the performance of the Work terminated by the notice of termination, and

40.3.6.2 the completed or partially completed plans, drawings, information, and other property which, if the Contract had been completed, would have been required to be furnished to the Purchaser;

40.3.7 use his best efforts to sell, in the manner, at the times, to the extent, and at the price or prices directed or authorised by the Contracting Authority, any property of the types referred to in Clause 40.3.6 above. However, the Contractor:

40.3.7.1 shall not be required to extend credit to any Buyer; and

40.3.7.2 may acquire any such property under the conditions prescribed by and at a price or prices approved by the Purchaser; and provided further that the proceeds of any such transfer or disposition shall be applied in reduction of any payments to be made by the Purchaser to the Contractor under this Contract or shall otherwise be credited to the price or cost of the Work or paid in such manner as the Contracting Authority may direct;

40.3.8 complete performance of such part of the Work as shall not have been terminated by the Notice of Termination; and

40.3.9 take such action as may be necessary, or as the Purchaser may direct, for the protection and preservation of the property related to this Contract which is in the possession of the Contractor and in which the Purchaser has or may acquire an interest.

40.4 The Contractor may submit to the Purchaser a list, certified as to quantity and quality, of any or all items of termination inventory not previously disposed of, exclusive of items the disposition of which has been directed or authorised by the Purchaser, and may request the Purchaser to remove such items or enter into a storage agreement covering the same; provided that the list submitted

shall be subject to verification by the Purchaser upon removal of the items, or if the items are stored, within forty-five (45) Days from the date of submission of the list, and any necessary adjustment to correct the list as submitted shall be made prior to final settlement.

40.5 After receipt of a notice of termination, the Contractor shall submit to the Purchaser his termination Claim for the Work covered by the notice of termination, in the form and with certification prescribed by the Purchaser. Such claim shall be submitted promptly but in no event later than six (6) months from the effective date of termination, unless one or more extensions are granted in writing by the Purchaser, upon request of the Contractor made in writing within such six-month period or authorised extension thereof. However, if the Purchaser determines that the facts justify such action, the Purchaser may receive and act upon any such termination claim at any time after such six-month period or any extension thereof. Upon failure of the Contractor to submit his termination claim within the time allowed, the Purchaser may determine on the basis of information available to him, the amount, if any, due to the Contractor by reason of the termination and shall thereupon pay to the Contractor the amount so determined.

40.6 Subject to the provisions of Clause 40.5, the Contractor and the Purchaser may agree upon the whole or any part of the amount or amounts to be paid to the Contractor by reason of the total or partial termination of Work pursuant to this Clause, which amount or amounts may include a reasonable allowance for profit on work done; provided that such agreed amount or amounts exclusive of settlement costs shall not exceed total Contract price as reduced by the amount of payments otherwise made and as further reduced by the Contract price of the Work not terminated. The Contract shall be amended accordingly and the Contractor shall be paid the amount agreed.

40.7 In the event of the failure of the Contractor and the Purchaser to agree as provided in Clause 40.6 upon the whole amount to be paid to the Contractor by reason of the termination of Work pursuant to Clause 40, the Purchaser shall pay to the Contractor the amounts determined by the Purchaser as follows, but without duplication of any amounts agreed upon in accordance with Clause 40.6 the total of:

40.7.1 for completed Work accepted by the Purchaser (or sold or acquired as provided in Clause 40.3 above) and not therefore paid for, a sum equivalent to the aggregate price for such Work computed in accordance with the price or prices specified in the Contract, appropriately adjusted for any saving of freight or other charges;

40.7.2 the costs incurred in the performance of the Work terminated including initial costs and preparatory expense allocable thereto, but exclusive of any costs attributable

to Work paid or to be paid for under Clause 40.7.1;

40.7.3 the cost of settling and paying claims arising out of the termination of work under Sub-contracts or orders, as provided in Clause 40.3.5, which are properly chargeable to the terminated portion of the Contract, exclusive of amounts paid or payable on account of Work or materials delivered or services furnished by Sub-contractors or vendors prior to the effective date of the notice of termination, which amounts shall be included in the costs payable under Clause 40.7.2; and

40.7.4 a sum, as profit on Clause 40.7.1 above, determined by the Purchaser to be fair and reasonable; provided, however, that if it appears that the Contractor would have sustained a loss on the entire Contract, had it been completed, no profit shall be included or allowed and an appropriate adjustment shall be made reducing the amount of the settlement to reflect the indicated rate of loss; and

40.7.5 the reasonable costs of settlement, including accounting, legal, clerical and other expenses reasonably necessary for the preparation of settlement claims and supporting data with respect to the terminated portion of the Contract and for the termination and settlement of Sub-contracts there under, together with reasonable storage, transportation, and other costs incurred in connection with the protection, or disposition of property allocable to this Contract.

40.8 The total sum to be paid to the Contractor under Clause 40.7 shall not exceed the total Contract price as reduced by the amount of payments otherwise made and as further reduced by the Contract price of Work not terminated.

40.9 Except for normal spoilage, and except to the extent that the Purchaser shall have otherwise expressly assumed the risk of loss, there shall be excluded from the amounts payable to the Contractor, as provided in Clause 40.7 above, the fair value, as determined by the Purchaser, of property which is destroyed, lost, stolen, or damaged so as to become undeliverable to the Purchaser, or to a buyer pursuant to Clause 40.3.7 above.

40.10 The Contractor shall have the right to dispute, under the Clause 41 (Disputes), any determination made by the Purchaser under Clauses 40.5 and 40.7, except that if the Contractor has failed to submit his claim within the time provided in Clause 40.5 and has failed to request extension of such time, the Contractor shall be foreclosed from his right to dispute said determination. In

any case where the Purchaser has made a determination of the amount due under Clauses 40.5 and 40.7, the Purchaser shall pay the Contractor the following:

40.10.1 if there is no right of appeal hereunder or if no timely appeal has been taken, the amount so determined by the Purchaser, or

40.10.2 if an appeal has been taken, the amount finally determined on such appeal.

40.11 In arriving at the amount due to the Contractor under this Clause there shall be deducted:

40.11.1 all unliquidated advance or other payments on account theretofore made to the Contractor, applicable to the terminated portion of this Contract;

40.11.2 any claim which the Purchaser may have against the Contractor in connection with this Contract; and

40.11.3 the agreed price for, or the proceeds of the sale of, any materials, Work, or other things acquired by the Contractor or sold, pursuant to the provisions of this Clause, and not otherwise recovered by or credited to the Purchaser.

40.12 If the termination hereunder is partial, prior to the settlement of the terminated portion of this Contract, the Contractor may file with the Purchaser, in accordance with Clause 16 (Changes), a request in writing for an equitable adjustment of the price or prices relating to the continued portion of the Contract (the portion not terminated by the notice of termination), and such equitable adjustment as may be agreed upon shall be made in such price or prices.

40.13 The Purchaser may from time to time, under such terms and conditions as it may prescribe, make partial payments and payments on account against costs incurred by the Contractor in connection with the terminated portion of this Contract whenever in the opinion of the Purchaser the aggregate of such payments shall be within the amount to which the Contractor will be entitled hereunder. If the total of such payment is in excess of the amount finally agreed or determined to be due under this Clause, such excess shall be payable by the Contractor to the Purchaser upon demand, together with interest calculated using the average of the official base rate(s) per annum of the deposit facility rate as notified by the European Central Bank or such other official source as may be determined by the Purchaser, for the period from the date the excess is received by the Contractor to the date such excess is repaid to the Purchaser, provided, however, that no interest shall be charged with respect to any such excess payment attributed to a reduction in the

Contractor's claim by reason of retention or other disposition of termination inventory until ten days after the date of such retention or disposition or such later date as determined by the Purchaser by reason of the circumstances.

40.14 Unless otherwise provided for in this Contract, the Contractor, from the effective date of termination and for a period of three years after final settlement under this Contract, shall preserve and make available to the Purchaser at all reasonable times at the office of the Contractor, but without direct charge to the Purchaser, all his books, records, documents, computer files and other evidence bearing on the costs and expenses of the Contractor under this Contract and relating to the work terminated hereunder, or, to the extent approved by the Purchaser, photographs, micro-photographs, or other authentic reproductions thereof.

41. DISPUTES

41.1 Except to the extent to which special provision is made elsewhere in the Contract, all disputes, differences or questions which are not disposed of by agreement between the Parties to the Contract with respect to any matter arising out of or relating to the Contract, other than a matter as to which the decision of the Contracting Authority under the Contract is said to be final and conclusive, shall be decided by the Contracting Authority. The Contracting Authority shall reduce his decision to writing and mail or otherwise furnish a copy thereof to the Contractor.

41.2 The Contracting Authority shall not proceed with the evaluation and decision in respect of any claim until and unless the Contractor has submitted the attestation as foreseen in Clause 18 (Claims), as well as the complete proof and evidence of the claim (either by submission or by identification of the relevant documentation).

41.3 The Contracting Authority's decision shall be final and conclusive unless, within 30 Days from the date of receipt of such copy, the Contractor mails or otherwise furnishes to the Contracting Authority his decision to open arbitration proceedings in accordance with the Clause 42 (Arbitration). The burden of proof for both receipt and delivery of such documentation shall be by signed and dated registered mail receipt or by hand receipt as acknowledged and signed by the Contracting Authority.

41.4 Pending final decision of a dispute, the Contractor shall proceed diligently with the performance of the Contract, unless otherwise instructed by the Contracting Authority.

42. ARBITRATION

42.1 Within a period of thirty days from the date of receipt of the notification referred to in Clause 41.3 above, the Parties shall jointly appoint an arbitrator. In the event of failure to appoint an arbitrator, the dispute or disputes shall be

submitted to an Arbitration Tribunal consisting of three arbitrators, one being appointed by the Purchaser, another by the other contracting party and the third, who shall act as President of the Tribunal, by these two arbitrators. Should one of the Parties fail to appoint an arbitrator during the fifteen days following the expiration of the first period of thirty days, or should the two arbitrators be unable to agree on the choice of the third member of the Arbitration Tribunal within thirty days following the expiration of the said first period, the appointment shall be made, within twenty-one days, at the request of the Party instituting the proceedings, by the Secretary General of the Permanent Court of Arbitration at The Hague.

42.2 Regardless of the procedure concerning the appointment of this Arbitration Tribunal, the third arbitrator will have to be of a nationality different from the nationality of the other two members of the Tribunal.

42.3 Any arbitrator must be of the nationality of any one of the member states of NATO and shall be bound by the rules of security in force within NATO.

42.4 Any person appearing before the Arbitration Tribunal in the capacity of an expert witness shall, if he is of the nationality of one of the member states of NATO, be bound by the rules of security in force within NATO. If he is of another nationality, no NATO classified documents or information shall be communicated to him.

42.5 An arbitrator, who, for any reason whatsoever, ceases to act as an arbitrator, shall be replaced under the procedure laid down in Clause 42.1 above.

42.6 The Contractor agrees to submit to the Arbitration Tribunal only such issues, facts, evidence and proof which the Contractor had beforehand identified and submitted to the Contracting Authority for decision in accordance with Clause 41 (Disputes). The jurisdictional authority of the Arbitration Tribunal shall be restricted to consider only those identical issues, facts, evidence and proof so identified and submitted to the Contracting Authority.

42.7 The Purchaser likewise agrees to restrict its submissions only to the information on which the Contracting Authority based its decision and not to introduce new information and arguments which cannot reasonably be deduced or inferred from the written decision of the Contracting Authority in response to the original dispute.

42.8 The Arbitration Tribunal will take its decisions by a majority vote. It shall decide where it will meet and, unless it decides otherwise, shall follow the arbitration procedures of the International Chamber of Commerce in force at the date of signature of the present Contract.

42.9 The awards of the arbitrator or of the Arbitration Tribunal shall be final and there shall be no right of appeal or recourse of any kind. These awards shall

determine the apportionment of the arbitration expenses.

42.10 Pending final decision of a dispute, the Contractor shall proceed diligently with the performance of the Contract, unless otherwise instructed by the Contracting Authority.

43. SEVERABILITY

43.1 If one or more of the provisions of this Contract is declared to be invalid, illegal or unenforceable in any respect under any applicable law, the validity, legality and enforceability of the remaining provisions shall not be affected. Each of the Parties shall use its best efforts to immediately and in good faith negotiate a legally valid replacement provision.

44. APPLICABLE LAW

44.1 This Contract shall be governed, interpreted and construed in accordance with the private contract law of the Kingdom of Belgium.

* *

ANNEX 1 TO GENERAL PROVISONS: PURCHASER'S PRICING PRINCIPLES

A. General

1. With regard to all actions included in Clause 19," Pricing of Changes, Amendments and Claims", the Parties agree that the Purchaser's Pricing Principles contained herein shall govern.

2. As may be requested by the Purchaser, the Contractor shall provide documentation. that the standards or principles employed in the submission of cost or pricing data are in conformance with governing national policies and regulation. The Contractor, when submitting a price proposal based upon national standards and regulations, shall provide a point of contact within the national body governing such standards and regulations in order to allow Purchaser verification and audit.

3. Where such conformance cannot be demonstrated to the satisfaction of the Purchaser, the Purchaser's Pricing Principles will govern.

4. The Contractor shall clearly state whether national standards and rules or the Purchaser's Pricing Principles and formats are the basis for the price proposal.

5. Whether national standards or Purchaser pricing principles are applied, all cost and pricing data shall be verifiable, factual and include information reasonably required to explain the estimating process.

6. The Contractor shall also incorporate provisions corresponding to those mentioned herein in all sub-contracts, and shall require price and cost analysis provisions be included therein.

B. Purchaser's Pricing Principles

1. Allowable cost

A cost is allowable for consideration by the Purchaser if the following conditions are fulfilled:

(a) it is incurred specifically for the Contract or benefits both the Contract and other work or is necessary to the overall operation of the business although a direct relationship to any particular product or service cannot be established and is allocated to them in respective proportion according to the benefit received;

i. Direct Costs
A direct cost is any cost which can be identified specifically with a particular cost objective as generally accepted. Direct costs are not limited to items which are incorporated in the end product as material or labour.

ii. Indirect Costs

An indirect cost is one which is not readily subject to treatment as a direct cost. When presented these costs shall be accumulated in logical cost groupings in accordance with sound accounting principles and the Contractor's established practices. An indirect cost may be allocated to more than one final cost objective. An indirect cost shall not be allocated to a final cost objective if other costs incurred for the same purpose, in like circumstances, have been included as a direct cost of that or any other final cost objective. Such costs shall be presented as overhead rates and be applied to each related direct cost grouping.

(b) The Contractor shall specify the allocation of costs to either of the cost groupings. The method by which costs are accumulated and distributed as part of direct or indirect costs cannot be modified during the duration of the Contract.

(c) it is reasonable and expedient in its nature and amount and does not exceed that which would be incurred by an ordinary prudent person in the conduct of competitive business;

(d) it is not liable to any limitations or exclusion as to types or amounts of cost items as set forth herein.

(e) The Purchaser will review other costs presented against the contract and will determine if they would be allowable.

2. Unallowable Costs

In general all costs which cannot be shown by the contractor to be directly or indirectly of benefit to the Contract are totally unallowable. =Examples of such costs are, among others:

(a) Advertising costs

(b) Costs of remuneration, having the nature of profit sharing.

(c) Costs of maintaining, repairing and housing idle and excess facilities.

(d) Fines and penalties as well as legal and administrative expenses resulting from a violation of laws and regulations.

(e) Losses on other contracts or on expected follow-on contracts

(f) Costs incurred for the creation of reserves for general contingencies or other reserves (e.g. for bad debts, including losses).

(g) Losses on bad debts, including legal expenses and collection costs in connection with bad debts.

(h) Costs incurred to raise capital.

(i) Gains and losses of any nature arising from the sale or exchange of capital assets other than depreciable property.

(j) Taxes on profits.

(k) Contractual penalties incurred.

(l) Commissions and gratuities.

(m) Interest on borrowings.

3. Rates and Factors

(a) The Contractor shall inform the Purchaser of his rates and factors the basis upon which they were computed.

(b) If the Contractor's rates and factors for similar contracts placed with national or international public services have not been established or approved by a government agency or an agency accepted by his government, the Contractor shall provide the necessary data to support the proposed rates.

(c) The term "provisional " used in the title of a rate or factor means a tentative rate established for interim billing purposes pending negotiation and agreement to the final rate or factor.

(d) A rate or factor is pre-determined if it is fixed before or during a certain period and based on (estimated) costs to be incurred during this period. An rate or factor is post-determined if it is fixed after a certain period and based on costs actually incurred during this period. Pre-determined rates or factors shall be agreed upon as final rates whenever possible; otherwise the provisions of paragraph 3c above shall apply pending agreement to post-determined rates or factors.

(e) Such rates or factors shall be determined on the basis of Contractor's properly supported actual cost experience.

(f) If the rates or factors of the Contractor for similar contracts placed by national or international public services have been established or approved by a government agency or an agency accepted by his government and the Contractor proposes the application of these rates, he shall state the name and address of the agency which has accepted or approved the rates and the period for which they were established. If he proposes rates which vary from the rates mentioned above, he shall furthermore provide a justification for the difference.

4. Profit/Benefit

(a) Over the entire life cycle of a given acquisition, Profit and/or Benefit may be subject to negotiation.

(b) Subcontracting profit/benefit amounts are dependent upon the size, nature and oversight needs of the subcontract(s) the prime contractor will use for work performance period.

(c) Profit/benefit is considered by the Purchaser to be directly related to the anticipated risk of the Contractor during the performance of the Contract.

INFORMATION EXCHANGE GATEWAY (IEG) SOLUTIONS BETWEEN NATO SECRET AND NATO-LED MISSION SECRET DOMAINS

IFB-CO-14314-IEG-C

BOOK II - PART IV

STATEMENT OF WORK (SOW)

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

SECTION 1: INTRODUCTION

1.1. Purpose

1.1.1. NATO requires a data loss prevention capability, to prevent the unauthorised release of data from the NATO SECRET to a NATO/xFOR SECRET domain. The aim of this procurement project is to industrialize the existing prototype capabilities, thereby reducing risks to security, providing resilience, improving control, management and maintenance aspects, while adhering to newly approved NATO Standards.

1.1.2. The Information Exchange Gateway Scenario C (hereafter called IEG-C) project will provide:

1.1.2.1. Support for Information Exchange Services of information and real time data between the NATO Secret core network (which comprise NATO Commands, Agencies, and connected NATO Nations) and NATO/xFOR Secret networks (for NATO Responses Forces, NATO-led Coalition Exercises and Operations).

1.1.2.2. These services will be provided by a gateway system, which should be able to scale based on the needs of the supported mission, available bandwidth and required response times.

1.1.2.3. These gateways may be in deployed locations but will be centrally managed, monitored and controlled, while physical maintenance will be undertaken by local staff.

1.1.2.4. The main objective of the gateway is to protect NATO Secret (NS) information and CIS while supporting the required interactions between the NS and mission secret CIS. The gateway will mediate exchange of data for both ‘core’ and ‘functional’ services and will, whenever possible, conform to NATO Standardization Agreements (STANAGs) 4774 and 4778[1].

[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.*

1.2. System Description

[1] References provided in Section 2

1.2.1. The IEG-C is a Data Loss Prevention bi-directional guard at the interface between the (or "a") NATO SECRET (NS) domain and a NATO-led 'mission' domain, such as 'Resolute Support' or 'KFOR'. The guard approves or rejects the transmission of data between the two security domains based on either a STANAG-compliant trusted classification label, such as 'NATO <classification> Releasable to <mission>' or trusted source to trusted destination mediated by firewall rule sets. The reason for the trusted source/destination path is that not all current NATO services and apps are 'label aware'.

1.2.2. The overall requirement for the IEG-C is to allow a mission command structure to operate the full range of military command and control IT functions where the staff and users include NATO and non-NATO mission partners. All non-NATO mission partners will have security agreements with NATO such that they are authorised to access information classified up to NATO SECRET Releasable to <Mission>. In such a situation, two IT systems are provided; one classified 'NATO SECRET' to process information that is required for the mission but not releasable to non-NATO partners (typically J2 data) and one classified <Mission> SECRET that is accessible to all authorised mission partners, both NATO and non-NATO. For practical purposes, the majority of users are typically provided with access to the mission IT system. Users in the NS domain (both local and in the static NS domain) can be granted access to services and data in the <Mission> SECRET domain, but users in the <Mission> SECRET domain are prevented from any access to the NS domain.

1.2.3. The NATO requirement for users with elevated privileges (e.g. system administrators) to have a security clearance higher than the level of the system they operate means that only NATO cleared users can be granted such permissions. Where both NS and <Mission> SECRET IT systems are provided, data transfer requirements typically require the IEG-C to be deployed to the mission HQ so that LAN-level transfer speeds can be provided between the two IT systems. Where a mission has no NS component, the IEG-C can be located at the supporting HQ at the reach-back or mission anchor location. Possible configurations are shown below in Figure 1: IEG-C Modes of Operation:

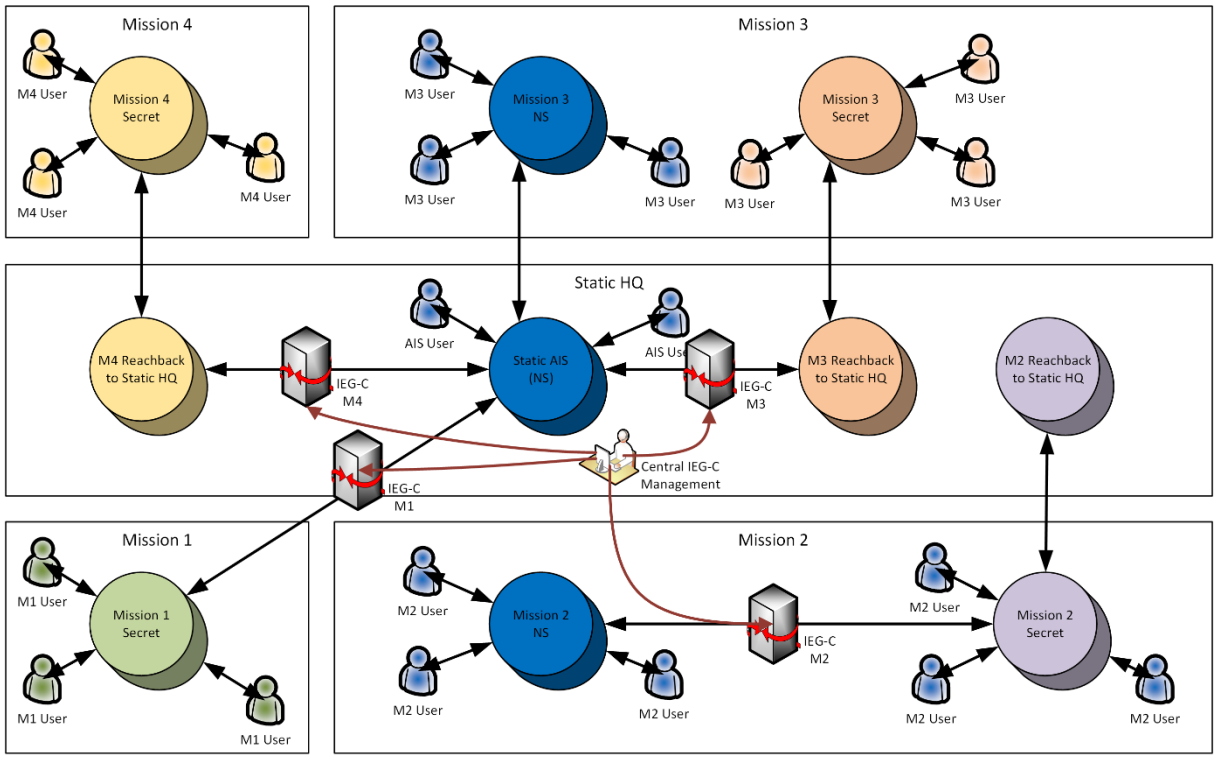

Figure 1: IEG-C Modes of Operation

1.2.4. The IEG-C requirement and operational prototype solutions have evolved over many years to a situation where there are two main variants in operation today; those with a 'DMZ' and those without. In the 'without' case, a firewall and a mail guard are connected in parallel between the two security domains. The 'DMZ' configuration adds a third domain mediated by the firewall that contains the mail guard and other guards and proxies, such as an XML web-guard and web reverse proxy.

1.2.5. The objective of the IEG-C project is to modernise and standardise the configurations to a single layout with a consolidated management suite like below in Figure 2: IEG-C Components and to add additional features required by, for instance, evolving security protection measures. It should be noted that configurations will never be fully identical as different missions will always operate different C2 tools and information exchange requirements due to the nature of the operation (Maritime-based, Land-based etc.). So there will be differences in the firewall rule sets and, of course, all missions have specific releasability labels.

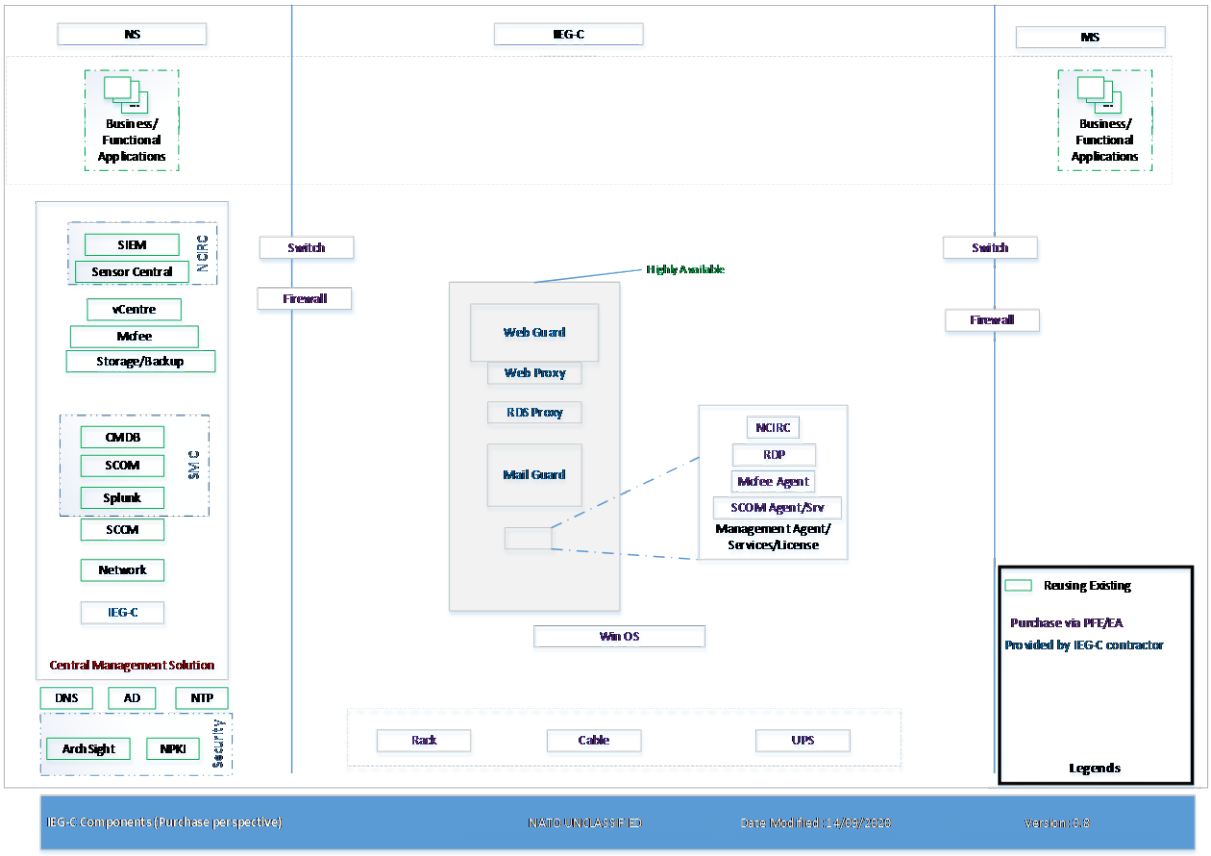

Figure 2: IEG-C Components

1.2.6. As the IEG-C is a data release guard, it does not support any on-line users and, other than log files, only supports transient data. All of the IEG-C components will be centrally managed by a Border Protection Services management team from a central location.

1.2.7. The logical layout and data flows of the IEG-C is shown below in Figure 3: IEG-C Data Flows. Features to note are that physically separate firewalls are required for the interface to the NS domain and the interface to the <Mission> SECRET domain and that separate IEG-Cs are required for each mission. The diagram is illustrative of the data flows between the NS and <Mission> SECRET domain and shows both operational and management streams.

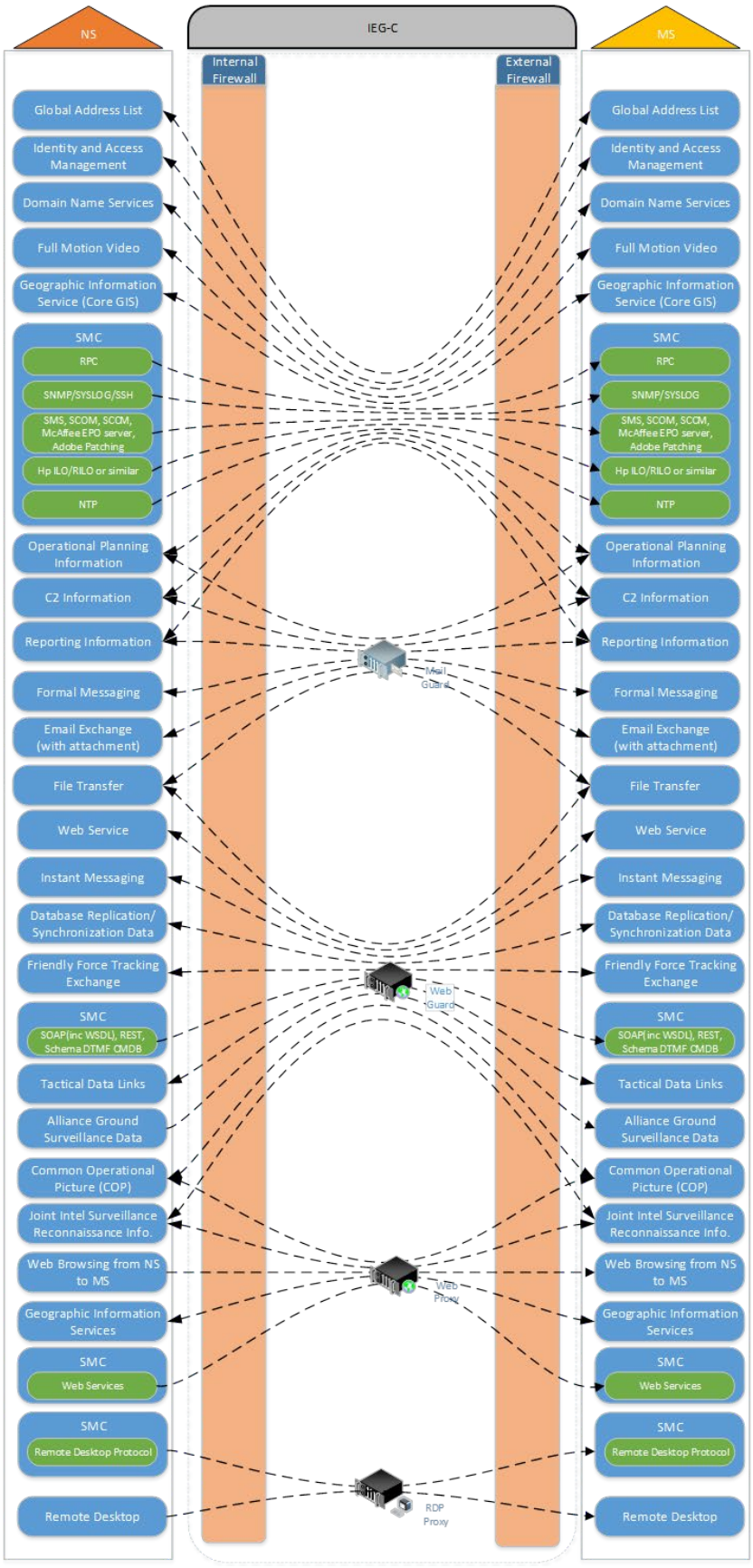

Figure 3: IEG-C Data Flows

1.3. Scope

1.3.1. The project will implement eleven (11) IEG-C systems in seven (7) locations (listed in Annex B.1), where prototype gateways have been already installed to meet NATO requirements for boundary protection, including one (1) reference system and a management facility to be installed in the first location in the NCI Agency at SHAPE.

1.3.2. The project may also implement optional installations (7 IEG-C systems in 7 locations). Six (6) of these options will be exercised depending on NATO future operational requirements and the 7th one, a virtualized instance, will be exercised when funding and specifications finalize to support NCIA IV&V activities. Options are described in SECTION 16.

1.3.3. Finally the project will remove the legacy prototypes it intends to replace, including those in 3 locations that will not receive new gateways.

1.3.4. This Statement of Work (SOW) describes requirements, as well as development, delivery and implementation processes for the IEG-C through a series of work packages as shown below in Table 1:

Number[2]	Name
2	Phase 1 Initial Design and Build
2.1	Design and Build to Factory Acceptance
2.2	Installation of the Reference System
2.3	Integration into NATO Enterprise and Management Capability
3	Installation of Operational Gateways
4	Decommissioning legacy gateways (3 sites)
	OPTIONS (NOT EVALUATED)
6	Hardware
7	Cyber Security Monitoring (former NCIRC)

Table 1: Work Packages

[SOW-2] *The Contractor SHALL deliver the **IEG-C** as detailed in the System Requirement Specifications (SRS).*

[2] WP1 was for the IEG-C Target architecture and is already executed

1.3.5. This Statement of Work (SOW) describes the responsibilities of and activities to be conducted by the Contractor to meet the requirements of the IEG-C project.

[SOW-3] *The Contractor SHALL provide all necessary resources to include services, personnel, materials, components, equipment[3], data[4] 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-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-5] *The Contractor SHALL be aware and comply with above mentioned documents throughout the Contract.*

1.3.6. Except otherwise stated, the delivery dates of the associated deliverables are provided in the Schedule of Supplies and Services (SSS) document.

[SOW-6] *The Contractor SHALL provide project management services.*

[SOW-7] *The Contractor SHALL provide systems engineering services to cover:*

- *Requirements review;*
- *System design and*
- *System Integration.*

[SOW-8] *The Contractor SHALL provide test, verification and validation services to prove the system Product Baseline is meeting its requirements.*

[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-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-11] *The Contractor SHALL provide System Services as described in SECTION 7*

[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-13] *The Contractor SHALL procure and prepare the system components, as agreed in this contract, for delivery to the sites specified in this Contract.*

---

[3] Required equipment will be identified by the bidders to conform to SRS, but part thereof may be provided by the customer as Purchaser Furnished Equipment (PFE). Lists will be finalized in PDR milestone (PRM 2, EDC+3). Detailed instructions are provided at 16.2 WP 6 Hardware.

[4] NATO specific data required for System or Component Configuration will be provided by the NCI Agency

[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-15] *The Contractor SHALL provide support to application and service management integration*

[SOW-16] *The Contractor SHALL provide Integrated Logistics Support (ILS), including training services, as described in SECTION 6 Integrated Logistics Support (ILS).*

[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-18] *The Contractor SHALL comply with all overarching requirements as described in the SOW (Testing process, Site survey process, Quality Assurance, Configuration Management).*

[SOW-19] *The Contractor SHALL meet or "exceed" the Notional schedule (see 3.2: Notional schedule).*

1.4. IEG-C Solution Constraints

1.4.1. The project will include a number of optional sites, to be confirmed at a later stage, depending on future operational requirements.

1.4.2. The aforementioned IEG-C Services shall include in particular, but will not be limited to:

- Text Chat
- Electronic mail
- Directory Services
- Web Services
- Common Operational Picture Data
- Tactical Data Links data
- Remote desktop services
- Video streams

1.4.3. IEG-C will utilise certificates provided by the NATO Public Key Infrastructure (NPKI) service.

1.4.4. The IEG-C as a system integrated in the NATO Enterprise infrastructure shall allow for automatic and seamless failover between multiple IEG-C gateways properly setup.

1.4.5. The IEG-C as a system integrated in the NATO Enterprise infrastructure shall allow for

1.4.6. Security enforcing products shall be evaluated in accordance with NATO Security Policy and supporting directives.

1.5. Statement of Work (SOW) organisation

1.5.1. This SOW describes the responsibilities of and activities to be conducted by the Contractor to meet the requirements of the IEG-C project.

1.5.2. Section Relevance

1.5.2.1. SECTION 2 defines the applicable documents.

1.5.2.2. SECTION 3 to SECTION 15, as well as the Annexes, define requirements of this Contract.

1.5.3. SECTION 16 describes the Options of this Contract.

1.5.4. Standards for Interpretation of the SOW:

1.5.4.1. The use of shall, should and will is defined as follows:

1.5.4.1.1. SHALL: This requirement is mandatory and must be implemented by the contractor.

1.5.4.1.2. SHALL NOT: means that the definition is an absolute prohibition of the specification.

1.5.4.1.3. WILL: This term is not implemented within the System Requirements Specification (SRS) requirements.

1.5.4.1.4. SHOULD: This term is implemented within the SRS requirements.

1.5.4.2. The words “preliminary” or “initial” or “first draft” for documents referenced in this SOW that need to be produced by the Contractor mean a document at 60% or more maturity.

1.5.4.3. This SOW invokes a variety of Standard NATO Agreements (STANAG), Allied Quality Assurance Publications (AQAPs), and Military Standards (MIL-STD). While these are NATO reference documents, there are national and international standards that are considered to be equivalent and are cited as such within these documents.

1.5.4.4. Where a national or international standard exists that is not specifically referenced in the STANAGs (and underpinning documents) or MIL-STDs as being equivalent, the Contractor may propose to utilise such a standard if he can demonstrate to the satisfaction of the Purchaser that such a standard is equivalent to the STANAGs or MIL-STD in question.

1.5.4.5. The Purchaser, however, reserves the right to deny such a request and demand performance in accordance with the standard cited in the SOW.

1.5.5. An Overall Project Schedule is provided in Section 3.2.

SECTION 2: APPLICABLE DOCUMENTS

[SOW-20] *The Contractor SHALL be aware and comply with the documents listed in SECTION 2 throughout the Contract.*

2.1. NATO Documents

2.1.1. Security Documents

Abbreviation	Full document Name and Reference
AC/322-D/0030-REV5	INFOSEC Technical & Implementation Directive for the Interconnection of Communication and Information Systems (CIS)
AC/322-D/0047-REV2 (INV)	"INFOSEC Technical & Implementation Directive On Cryptographic Security And Cryptographic Mechanisms"
AC/322-D(2017)0016 (INV)	Technical and Implementation Directive on Supply Chain Security for COTS CIS Security Enforcing Products
AC/322-N(2014)0158-ADD3	Selection and Installation of Equipment for the Processing of Classified Information
AD 070-005	ACO Communication and Information Systems (CIS) Security
AC/35-D/1017-REV3	Guidelines for Security Risk Management of CIS
AC/35-D/1021-REV3	Guidelines for the security accreditation of communication and information systems (CIS), 31 January 2012
AC/35-D/2004-REV3	Primary Directive on CIS Security, 15 November 2013
AC/35-D/2005-REV3	Management Directive on CIS Security
AC/322-D(2004)0030	INFOSEC Technical And Implementation Directive on the Requirement for, and the Selection, Approval and Implementation of, Security Tools (ST)
NS Reference Baseline	NATO SECRET CIS Security Reference Baseline – Security Mechanisms (SMs) Requirements for Core and Site Services
AC/322-D/0048-REV3	Technical and Implementation Directive on CIS Security
C-M(2002)49-COR12	Security Within The North Atlantic Treaty Organisation
AC/35-D/1030, 2005	Guidelines on Physical Security
AC/35-D/1014-REV3	Guidelines for the Structure and Content of Security Operating Procedures
AC/35-D/2001-REV3	Directive on Physical Security
AC/35-D/2002-REV5	Directive on the Security of NATO Classified Information
SDIP-27/2	NATO TEMPEST Requirements and Evaluation Procedures
SDIP-28/1	NATO Zoning Procedures

SDIP-29/2	Selection and Installation of Equipment for the Processing of Classified Information

2.1.2. Quality Assurance Documents

Abbreviation	Full document Name and Reference
STANAG 4107 – Edition 11	Mutual Acceptance of Government Quality Assurance and Usage of the Allied Quality Assurance Publications (AQAP) Edition 11, dated 16 Jan 19, and underpinning AQAPs

2.1.3. Configuration Management Documents

Abbreviation	Full document Name and Reference
STANAG 4427 – Edition 3	Configuration Management In System Lifecycle Management – ACMP-2000 edition A & ACMP-2009 Edition A & ACMP-2100 Edition A, dated 18 Dec 14, and underpinning Allied Configuration Management Publications (ACMPs)
NCI Agency AI 06.03.01, 2015	NATO Communications and Information Agency - Agency Instruction 06.03.01, "Identification of Software Assets", 2015

2.1.4. Technical Guidance

Abbreviation	Full document Name and Reference
FMN SI Informal Messaging	FMN Spiral 1 Service Instructions for Informal Messaging, 18th February 2016
INSTR TECH 06.02.01	Service Interface Profile for Security Services, 4th February 2015
INSTR TECH 06.02.02	Service Interface Profile for REST Security Services, 4th February 2015
INSTR TECH 06.02.06	Service Interface Profile for Messaging (SOAP), 4th February 2015
INSTR TECH 06.02.07	Service Interface Profile for REST Messaging, 4th February 2015
NAC AC/322-D(2004)0019(INV), 2004	North Atlantic Council Document AC/322-D(2004)0019(INV), “INFOSEC Technical and Implementation Guidance for the Protection of CIS from Malicious Software”, March 2004
AC/322-D(2004)0024-REV3-COR1, 2018	North Atlantic Council Document AC/322-D(2004)0024-REV3-COR1 “CIS Security Technical And Implementation Directive On The NATO PKI Certificate Policy”, April 2018
AC/322-D(2007)0002-REV1, 2015	North Atlantic Council Document AC/322-D(2007)0002-REV1, “CIS Security Technical And Implementation Guidance in

	Support of Public Key Infrastructure - Cryptographic Aspects", March 2015
AC/35-D/1032, 2005	North Atlantic Council Document AC/35-D/1032, 2005 "Guidelines on the Security of Information", May 2005
NCIA RD-3381, 2012	NATO Communications and Information Agency, Reference Document 3381, "High Level Design for the NATO High Assurance Automated Guard", April 2012
NCIA TN-1485 v1.1, 2012	NATO Communications and Information Agency, "Common Criteria (CC) Protection Profile (PP) for a Medium Assurance NATO XML-Labelling Guard, Version 1.1", K. Wrona, S. Oudkerk, December 2012
NC3A TN-1486, 2012	NATO Consultation, Command and Control Agency Technical Note 1486, "NATO Content Inspection Policy Enforcement Framework Functional Specification", A. Ross, S. Oudkerk, April 2012.
NC3B AC/322-D(2019)0034 (INV), 2019	NATO C3 Board AC/322-D(2019)0034 (INV), "C3 Taxonomy Perspective Baseline 23.1", 2019
NCIA SMC TA, 2018	NATO Communications and Information Agency, "Target Architecture - Enterprise Service Management and Control", 2018
NCIA TR-2012-SPW008418-29, 2014	NATO Communications and Information Agency , "Cryptographic Access Control In Support Of Object Level Protection", S. Oudkerk, K Wrona, February 2014
NCIA TR/2016/NSE010871/01, 2017	NATO Communications and Information Agency , , "Information Exchange Gateway Scenario C Phase 1: Target Architecture – Final", IEG-C Team, January 2017
[NCI Agency TR/2017/NCB010400/12, 2017]	NATO Communications and Information (NCI) Agency Technical Report 2017/NCB010400/12, "NATO Enterprise Security Monitoring Guidance Version 1.0", Sébastien Gay, Philippe Lagadec, Jean-Francois Agneessens, Nikolaos Virvilis-Kollitiris, NCI Agency, The Hague, The Netherlands, June 2017 (NATO RESTRICTED).
NAC AC/322-D(2012)0022, 2013	North Atlantic Council, Consultation Command and Control Board (C3B)"Technical Implementation Guidance on Cryptographic Mechanisms in Support of Cryptographic Services", January 2013 (NATO RESTRICTED)

2.1.5. Standard Guidance

Abbreviation	Full document Name and Reference
STANAG 1059	Letter Codes for Geographical Entities
STANAG 4774	Confidentiality Metadata Label Syntax
STANAG 4778	Metadata Binding Mechanism

STANAG 4778 SRD.2	Standard Related Document SRD.2 “Binding Profiles
NATO STANAG 6001, 2014	NATO Standardisation Agreement 6001, "Language Proficiency Levels", Ed. 5, 2014
MILSTD810, 2000	Environmental Engineering Considerations and Laboratory Tests
AECTP300, 1998	Climatic Environmental Tests
MILSTD461E, 1999	EMC Testing

2.1.6. NATO Templates

Abbreviation	**Full document Name and Reference**
[NTEMP-1]	Interface Control Document template
[SRA template]	Security Risk Assessment (SRA) Report template
[STVR template]	Security Test and Verification Report template
[SISRS template]	System Interconnection Security Requirements Statement (SISRS) template
[STVP template]	

2.1.7. Others

Abbreviation	**Full document Name and Reference**
IEG-C description	Information Exchange Gateway Scenario C (IEG-C) description
IEG-C SAP	NATO Security Accreditation Plan (SAP) for Information Exchange Gateway Scenario C (IEG-C)
NATO VIG v3	NATO Visual Identity Guidelines Version 3 (online: https://www.nato.int/vigs/pdf/NATO-VIGs-2016-en.pdf)

2.2. **Non-NATO Documents**

Abbreviation	**Full document Name and Reference**
AIA/ASD SX000i, 2016	Aerospace Industries Association/Aerospace and Defence Industries Association of Europe SX000i, "International guide for the use of the S-Series Integrated Logistic Support (ILS) specifications (issue 1.1)", 2016
AIA/ASD S3000L, 2014	Aerospace Industries Association/Aerospace and Defence Industries Association of Europe S3000L - International specification for Logistics Support Analysis – LSA (issue 1.1), 2014
EVM Practice Standard	Practice Standard for Earned Value Management (2011), Project Management Institute

IETF RFC 791, 1981	Internet Engineering Task Force (IETF) Request For Comments (RFC) 791, “Internet Protocol, DARPA Internet Program Protocol Specification”, September 1981.
IETF RFC 854, 1983	Internet Engineering Task Force (IETF) Request For Comments (RFC) 854, “Telnet Protocol Specification”, May, 1983
IETF RFC 959, 1985	Internet Engineering Task Force (IETF) Request For Comments (RFC) 959, “File Transfer Protocol (FTP)”, October 1985
IETF RFC 1983, 1996	Internet Engineering Task Force (IETF) Request For Comments (RFC) 1983, “Internet Users' Glossary”, August 1996
IETF RFC 2119, 1997	Internet Engineering Task Force Request for Comments 2119, "Key Words for Use in RFCs to Indicate Requirement Levels", 1997
IETF RFC 2312, 1998	Internet Engineering Task Force (IETF) Request For Comments (RFC) 2312, “S/MIME Version 2 Certificate Handling”, March 1998.
IETF RFC 2789, 2000	Internet Engineering Task Force (IETF) Request For Comments (RFC) 2789, “Mail Monitoring MIB”, March 2000.
IETF RFC 2818, 2000	Internet Engineering Task Force (IETF) Request For Comments (RFC) 2818, “HTTP Over TLS”, May 2000.
IETF RFC 2865, 2000	Internet Engineering Task Force (IETF) Request For Comments (RFC) 2865, “Remote Authentication Dial In User Service (RADIUS)”, June 2000.
IETF RFC 3339, 2000	Internet Engineering Task Force (IETF) Request For Comments (RFC) 3339, “Date and Time on the Internet: Timestamps”, July 2002.
IETF RFC 3410 – 3418, 2002	Internet Engineering Task Force (IETF) Request For Comments (RFC) 3410 through 3418, “S/MIME Version 2 Certificate Handling Introduction and Applicability Statements for Internet Standard Management Framework”, December 2002.
IETF RFC 3461, 2003	Internet Engineering Task Force (IETF) Request For Comments (RFC) 3461, “Simple Mail Transfer Protocol (SMTP) Service Extension for Delivery Status Notifications (DSNs)”, January 2003.
IETF RFC 3464, 2003	Internet Engineering Task Force (IETF) Request For Comments (RFC) 3461, “An Extensible Message Format for Delivery Status Notifications”, January 2003”, January 2003.
IETF RFC 4251, 2006	Internet Engineering Task Force (IETF) Request For Comments (RFC) 4251, “The Secure Shell (SSH) Protocol Architecture”, January 2006.
IETF RFC 4253, 2006	Internet Engineering Task Force (IETF) Request For Comments (RFC) 4253, “The Secure Shell (SSH) Transport Layer Protocol”, January 2006.

IETF RFC 4510-4519, 2006	Internet Engineering Task Force (IETF) Request For Comments (RFC) 4510 through 4519, “Lightweight Directory Access Protocol (LDAP)”, June 2006.
IETF RFC 5280, 2008	Internet Engineering Task Force (IETF) Request For Comments (RFC) 5280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, May 2008.
IETF RFC 5321, 2008	Internet Engineering Task Force (IETF) Request For Comments (RFC) 5321, “Simple Mail Transfer Protocol”, October 2008.
IETF RFC 5322, 2008	Internet Engineering Task Force (IETF) Request For Comments (RFC) 5322, “Internet Message Format”, October 2008.
IETF RFC 5424, 2009	Internet Engineering Task Force (IETF) Request For Comments (RFC) 5424, “The Syslog Protocol”, March 2009.
IETF RFC 5652, 2009	Internet Engineering Task Force (IETF) Request For Comments (RFC) 5652, “Cryptographic Message Syntax (CMS)”, September 2009.
IETF RFC 6125, 2011	Internet Engineering Task Force (IETF) Request For Comments (RFC) 6125, “Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)”, March 2011.
IETF RFC 6353, 2011	Internet Engineering Task Force (IETF) Request For Comments (RFC) 6353, “”,
IETF RFC 6960, 2013	Internet Engineering Task Force (IETF) Request For Comments (RFC) 2818, “HTTP Over TLS”, May 2000.
IETF RFC 7030, 2013	Internet Engineering Task Force (IETF) Request For Comments (RFC) 7030, “Enrolment over Security Transport” (EST).
IETF RFC 7230, 2014	Internet Engineering Task Force (IETF) Request For Comments (RFC) 7230, “Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing”, June 2014.
IETF RFC 7231, 2014	Internet Engineering Task Force (IETF) Request For Comments (RFC) 7231, “Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content”, June 2014.
IETF RFC 7414, 2015	Internet Engineering Task Force (IETF) Request For Comments (RFC) 7414, “A Roadmap for Transmission Control Protocol (TCP) Specification Documents”, February 2015.
IETF RFC 7525, 2015	Internet Engineering Task Force (IETF) Request For Comments (RFC) 7525, “Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)”, May 2015
IETF RFC 7540, 2015	Internet Engineering Task Force (IETF) Request For Comments (RFC) 7540, “Hypertext Transfer Protocol Version 2 (HHTP/2)”, May 2015.
IETF RFC 7817, 2016	Internet Engineering Task Force (IETF) Request For Comments (RFC) 7817, “Updated Transport Layer Security (TLS) Server

	Identity Check Procedure for Email-Related Protocols", March 2016
IETF RFC 8200, 2017	Internet Engineering Task Force (IETF) Request For Comments (RFC) 2460, "Internet Protocol, Version 6 (IPv6) Specification", July 2017.
IETF RFC 8446, 2018	Internet Engineering Task Force (IETF) Request For Comments (RFC) 8446, "The Transport Layer Security (TLS) Protocol Version 1.3", August 2018.
IETF RFC 8550, 2019	Internet Engineering Task Force (IETF) Request For Comments (RFC) 8550, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Certificate Handling", April 2019.
IETF RFC 8551, 2019	Internet Engineering Task Force (IETF) Request For Comments (RFC) 8551, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification", April 2019.
IPMI V2.0, 2013	Intel, Hewlett-Packard, NEC, Dell "IPMI – Intelligent Platform Management Interface Specification Second Generation, v2.0" Document Revision 1.1, October 2013
ISO 9000, 2015	International Organization for Standardization 9000 Series, "Quality Management Principles (Version 2015)", 2015
ISO 10012, 2003	International Organization for Standardization 10012 (Version 2003), "Measurement Management Systems – Requirements for measurement processes and measuring equipment", 2003
ISO/IEC 12207, 2017	International Organization for Standardization/International Electrotechnical Commission 12207, "Information Technology – Software Lifecycle Processes", 2008
ISO/IEC 25010, 2011	International Organization for Standardization/International Electrotechnical Commission 25010, "Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models", 2011
ISO/IEC/IEEE 29119, 2013	International Organization for Standardization/International Electrotechnical Commission/Institute of Electrical and Electronics Engineers 29119-Part 1, "Concepts and definitions. Part 2 Test processes. Part 3 Test documentation", 2013
ISO/IEC 15408, v.3.1	Common Criteria for Information Technology Security Evaluation
ITIL v3, 2007	Office of Government Commerce, "Information Technology Infrastructure Library (ITIL) V.3", 2007
MIL-STD 882E, 2011	US Department of Defense Military Standard 882E, "System Safety", 2011
NIAP PP_APP_V.1.2, 2016	Protection Profile for Application Software Version 1.2
NIAP PP_OS_V.4.1, 2016	Protection Profile for General Purpose Operating Systems

NIAP CPP_FW_V.1.0, 2015	Collaborative Protection Profile for Stateful Traffic Filter Firewalls
NIAP CPP_ND_V.1.0,2015	Collaborative Protection Profile for Network Devices
NIAP PP_NDCP_IPP_EP_V .2.1, 2016	Collaborative Protection Profile for Network Devices/Collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package (EP) for Intrusion Prevention Systems (IPS)
NIAP PP_ESM_V.2.1, 2013	Standard Protection Profile for Enterprise Security Management Policy Management
NIAP PP_ESM_AC_V.2.1, 2013	• Standard Protection Profile for Enterprise Security Management Access Control
RDP Overview, 2019	“Remote Desktop Services Protocols Overview”, May 2019, available at: https://winprotocoldoc.blob.core.windows.net/productionwindowsarchives/MS-RDSOD/%5bMS-RDSOD%5d.pdf
W3C SOAP 1.1, 2000	World Wide Web Consortium, Note, “Simple Object Access Protocol (SOAP) 1.1”, May 2000
W3C SOAP 1.2, 2007	World Wide Web Consortium, Recommendation, “SOAP Version 1.2 Part 1: Messaging Framework”, April 2007
W3C Canonical XML Version 1,1, 2008	World Wide Web Consortium, Recommendation, “Canonical XML Version 1,1”, May 2008
W3C XML Schema 1.0, 2004	XML Schema Definition Language (XSD) 1.0, 2004
W3C XML Path Language 1.0, 1999	World Wide Web Consortium, Recommendation, “XML Path Language (XPath) Version 1.0”, 25 March 2003
W3C XPointer, 2003	World Wide Web Consortium, Recommendation, “XPointer Framework”, 25 March 2003

SECTION 3: MILESTONES

3.1. Introduction

3.1.1. This section provides a notional view of the project logical schedule as well as the list of key project milestones and criteria to be met by the Contractor to achieve them.

3.1.2. Key project milestones are defined as follows:

- Effective Date of Contract (EDC)
- System Requirements Review (SRR)
- Preliminary Design Review (PDR)
- Critical Design Review (CDR)
- Factory Acceptance Test (FAT)
- Acceptance of IEG-C security accreditation package
- System Integration Testing (SIT) + System Acceptance Testing (SAT)+User Acceptance Testing (UAT)
- Deployment Authorization (DA)
- Preliminary System Acceptance (PSA)
- Site Accreditation
- Site Acceptance Phase (SA)
- Operational Test & Evaluation (OT&E)
- Final System Acceptance (FSA)
- Decommissioning

[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).*

3.2. Notional schedule

Figure 3 provides the Overall Project Schedule with expected timeline for each Work Package. Each Work Package scope is defined in Annex B.2

3.2.1. Work Package Scope

3.2.2. Project will start with Effective Date of Contract (EDC) milestone.

[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).*

3.2.3. Effective Date of Contract (EDC)

[SOW-23] *The Effective Date of Contract (EDC) SHALL be established at the time of Contract Award (CAW).*

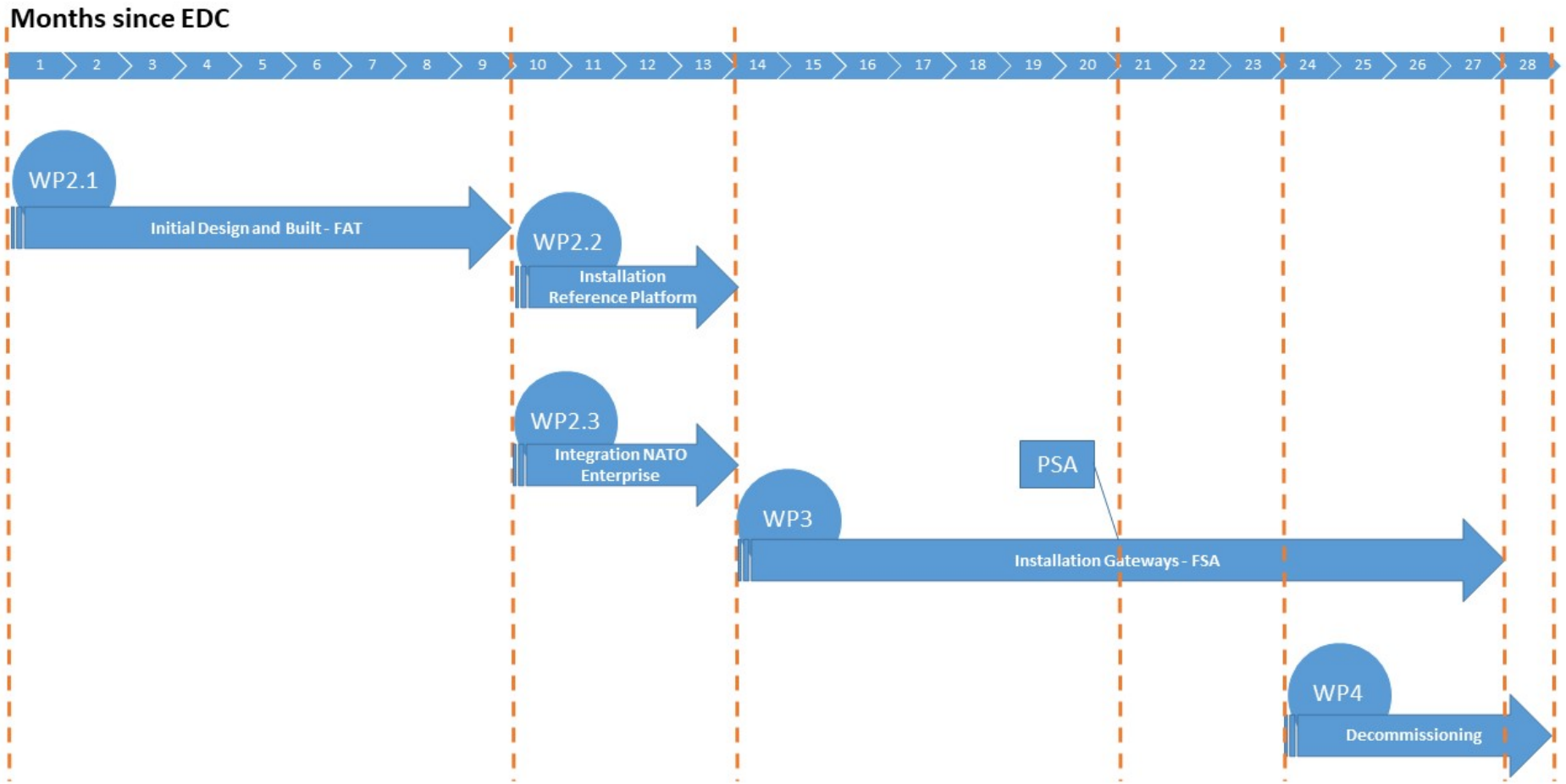

Figure 3: Overall Project Schedule

[SOW-24] *The Contractor SHALL integrate IEG-C in its Project Master Schedule at minimum by committing to deliver:*

- *System Requirements Review (SRR)*
- *Preliminary Design Review (PDR)*
- *Critical Design Review (CDR)*
- *Factory Acceptance Test (FAT)*
- *Acceptance of IEG-C security accreditation package*
- *System Integration Testing (SIT) + System Acceptance Testing (SAT)+User Acceptance Testing (UAT)*
- *Deployment Authorization (DA)*
- *Preliminary System Acceptance (PSA)*
- *Site Accreditation (security accreditation of interconnection via particular instance of IEG-C)*
- *Site Acceptance Phase (SA)*
- *Operational Test & Evaluation (OT&E)*
- *Final System Acceptance FSA*

Project Milestones

Milestone	No later than
Effective Date of Contract (EDC)	EDC
System Requirements Review (SRR)	EDC+2mo
Preliminary Design Review (PDR)	EDC+3mo
Critical Design Review (CDR)	EDC+6mo
Factory Acceptance Test (FAT)	EDC+9mo
Acceptance of IEG-C security accreditation package	EDC+13mo
System Integration Testing (SIT) + System Acceptance Testing (SAT)+User Acceptance Testing (UAT)	EDC+17mo
Deployment Authorization (DA)	EDC+20mo
Preliminary System Acceptance (PSA)	EDC+20mo
Site Accreditations	EDC+25mo
Site Acceptance Phase (SA)	EDC+25mo
Operational Test & Evaluation (OT&E)	EDC+26mo
Final System Acceptance FSA	EDC+27mo
Decommissioning	Up to 4 months after FSA

Table 2: Project Milestones

[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-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-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-28] *Upon the exercise of a contract option, the Contractor SHALL 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-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.*

3.3. System Requirements Review (SRR)

3.3.1. The System Requirements Review (SRR) is a multi-disciplined review to ensure that the system under review can proceed into initial systems development, and that all system requirements and performance requirements derived from the approved SRS are defined and testable, and are consistent with cost, schedule, risk, technology readiness, and other system constraints.

[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-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-32] *The Contractor SHALL review the Contractual **IEG-C** System Requirements Specification (SRS) and all other applicable documents, including:*

- *liaise with NATO subject matter experts as necessary;*
- *prepare its recommendations in terms of proposed changes to the System Requirements Specification (SRS);*
- *propose changes to the SRS (if any), in order to resolve inconsistencies and/or make improvements; such proposals will be considered by the Purchaser through the CCB process after Systems Requirements Review Meetings.*

[SOW-33] *The Contractor SHALL identify any inconsistencies within the requirements or that are in conflict (e.g. with design constraints).*

[SOW-34] *The Contractor SHALL justify any proposed changes to the requirements by the expected system cost, schedule, performance, and supportability impacts.*

[SOW-35] *The Contractor SHALL use as its SRS the Purchaser provided SRS with approved changes and, as required, extended with additional details supporting the approved scope.*

[SOW-36] *The Contractor SHALL deliver proposed changes to the SRS prior to SRR (EDC+2MO).*

3.3.2. SRR Entry Criteria

[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)*

Serial	Activities/Documents
1.	A preliminary SRR agenda
2.	Use Case documentation
3.	Success Criteria (enhanced or adapted)
4.	System Requirements Specification (SRS)
5.	Draft Security Risk Assessment Report (SRA-R)
6.	Draft System Interconnection Security Requirements Statements (SISRS)
7.	Preliminary system requirements allocation to the next lower levels.
8.	Updated schedule
9.	Preliminary software development plan
10.	Preliminary verification and validation approach
11.	Updated risk assessment and mitigations in the Risk Register
12.	Active Change Request (CR)

Table 3: The SRR Entry Criteria

[SOW-38] *The Contractor SHALL perform a System Requirements Analysis Review (see Section 5.3: System Requirements Analysis and Review).*

[SOW-39] *The Contractor SHALL update the Change Proposal documentation (see 12.6 Engineering Change Proposals (ECP)).*

3.3.3. The achievement of SRR is subject to the Purchaser approval which is based on accomplishment of the criteria listed in Table 4: The SRR Success Criteria

[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.*

Serial	Requirement
1.	The resulting overall concept is reasonable, feasible, complete, responsive to the operational requirements, and is consistent with system requirements and available resources (cost, schedule, staff, etc.).
2.	The project utilizes a sound process for the allocation and control of requirements throughout all levels, and a plan has been defined to complete the definition activity within schedule constraints. Preliminary software development plan exists
3.	Requirements definition, is complete with respect to the Contractual SRS requirements, and interfaces with external entities and between major internal elements have been defined
4.	Requirements allocation and traceability of key driving requirements have been defined from Contractual SRS, down to SRS and lower level system elements.
5.	System and element design approaches and operational concepts exist and are consistent with the SRS.
6.	The requirements, design approaches, and conceptual design will fulfil the mission needs within the estimated costs
7.	Preliminary approaches have been determined for how requirements will be verified and validated down to the system element level

8.	All changes to SRA, SRS, SISRS are agreed, they are accepted to have sufficient detail to begin or continue with the system design and implementation work
9.	Major risks have been identified, and viable mitigation strategies have been defined. Steps to mitigate risks are identified in the Risk Register

Table 4: The SRR Success Criteria

[SOW-41] *The Contractor SHALL consider the SRR 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.*

3.4. Preliminary Design Review (PDR)

3.4.1. The Preliminary Design Review (PDR at EDC+3MO) demonstrates that the preliminary design meets all system requirements with acceptable risk and within the cost and schedule constraints and establishes the basis for proceeding with detailed design. It will show that the correct design option has been selected, interfaces have been identified, and verification methods have been described.

[SOW-42] *Review and acceptance of design documentation provided by the Contractor to the Purchaser does not imply Purchaser acceptance of the design. The Contractor SHALL be solely responsible to prove the design through the regime of testing set forth in the Contract and the Contractor SHALL be solely responsible in the event that the system proves deficient in meeting the SRS*

[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-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-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-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-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.*

3.4.2. PDR Entry Criteria

[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*

Serial	Activities/Documents

1.	A preliminary PDR agenda
2.	Success Criteria (enhanced or adapted)
3.	Master Test Plan (MTP) (preliminary)
4.	Test Procedures/Test Cases (preliminary)
5.	System Design Specification (SDS) (preliminary)
6.	System Implementation Plan (SIP)
7.	Updated Security Risk Assessment Report (SRA-R)
8.	System Security Design Specification (SSDS) (preliminary)
9.	Requirements Traceability Matrix (RTM)
10.	Interface Control Description (ICD) (draft)
11.	Integrated Logistics Support Plan (ILSP) (draft)
12.	Updated Risk Register
13.	Active Change Requests

Table 5: The PDR Entry Criteria

3.4.3. The achievement of PDR is subject to the Purchaser approval which is based on accomplishment of the criteria listed in Table 6: The PDR Success Criteria

[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*

Serial	Requirement
1.	Agreement exists for the top-level requirements, including their verification and validation criteria, technical performance measures and any implementation constraints, and that these are finalised, stated clearly, and are consistent with the preliminary design
2.	The traceability of design artefacts to verifiable requirements is complete and proper or, if not, an adequate plan exists for timely resolution of open items. Design artefacts are traceable to the SRS.
3.	The preliminary design is expected to meet the requirements at an acceptable level of risk
4.	Definition of the technical interfaces is consistent with the overall technical maturity and proves an acceptable level of risk.
5.	Adequate technical interfaces are consistent with the overall technical maturity and provide an acceptable level of risk.
6.	Adequate technical margins exist with respect to technical performance measures
7.	The project and security risks are understood; plans, process and resources exist to effectively manage them. Steps to mitigate risks are identified in the Risk Register
8.	Major user interface features are reviewed and concept of interfaces are agreed.
9.	Non-functional requirements have been adequately addressed in preliminary designs.
10.	The operational concept is technically sound, that it includes (where appropriate) human factors that apply, and that requirements for its execution are traceable

Table 6: The PDR Success Criteria

3.5. Critical Design Review (CDR)

3.5.1. The purpose of the Critical Design Review (CDR at EDC+6MO) is to demonstrate that the maturity of the design is appropriate to support proceeding with full scale software and hardware implementation, integration, verification, validation and operation and that the technical effort is on track to complete system development in order to meet the SRS requirements within the identified cost and schedule constraints. At CDR the final version for each component (software) and interfaces to be used in the FBL shall be fixed. The Contractor will plan the CDR at the completion of the system design phase and conduct the CDR at the Purchaser's facility.

3.5.2. CDR Entry Criteria

[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)*

Serial	Activities/Documents
1.	A preliminary CDR agenda
2.	Success Criteria (enhanced or adapted)
3.	Successful completion of the PDR and responses has been made to all PDR open issues, or a timely closure plan exists for those remaining open.
4.	Master Test Plan (MTP) (final)
5.	Test Procedures/Test Cases (intermediate)
6.	Site Survey Reports
7.	Training Need Analysis (TNA)
8.	System Design Specification (SDS) (final)
9.	System Security Design Specification (SSDS) (final)
10.	Requirements Traceability Matrix (RTM) (update)
11.	Interface Control Description (ICD) (initial version)
12.	Integrated Logistics Support Plan (ILSP) (initial version)
13.	Updated Risk Register
14.	Active Change Requests

Table 7: The CDR Entry Criteria

[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-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-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-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.*

3.5.3. The achievement of CDR is subject to the Purchaser approval which is based on accomplishment of the criteria listed in Table 8: The CDR Success Criteria

[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.*

Serial	Requirement
1.	The detailed design is expected to meet the requirements with adequate margins at an acceptable level of risk. System Element-level functionality, design and interfaces are defined
2.	Core Services integration (at Service-level and host environment-level) is defined.
3.	System security, including Technical Services access-control mechanisms, data protection, backup and recovery, audit, interconnection, and information exchange security in context of the Services breakdown are defined.
4.	High-level design of Information Entities is completed.
5.	ICDs and SIPs are appropriately matured to proceed with implementation, integration and test, and plans are in place to manage any open items. System-level and Service-level interfaces, including external Services interfaces are defined.
6.	High confidence exists in the CDR, and adequate documentation exists and/or will exist in a timely manner to allow proceeding with implementation, integration, and test. For any elements that require development, the development methodology and documentation approach are defined
7.	Overall system design and its interactions, Services, components and Human-Machine Interface and Human Factors justifications are defined.
8.	For COTS products, the intended product and version, and note if any modifications, adaptations, or additional elements (such as macros or plug-ins) are required. Open Source Software (OSS) are to be disclosed (for review of OSS conditions by the Purchaser).
9.	The verification and validation requirements and plans are complete.
10.	The testing approach is comprehensive, and the planning for system integration, test, and operation is sufficient to progress into the next phase. Sequence and scope of system tests of each Baseline and any requirements for Purchaser support and participation are defined.
11.	Adequate technical and programmatic margins and resources exist to complete the development within budget, schedule, and risk constraints.
12.	Risks are understood, and plans and resources exist to effectively manage them. Steps to mitigate risks are identified in the Risk Register
13.	Non-functional requirements have been adequately addressed in system and operational designs.

Table 8: The CDR Success Criteria

3.6. Factory Acceptance Test (FAT)

[SOW-56] *The Contractor SHALL have performed necessary activities and satisfied criteria for meeting FAT (EDC+9MO) milestones as defined in SECTION 8 and SHALL achieve Purchaser approval of the associated documentation.*

3.7. Acceptance of IEG-C security accreditation package

[SOW-57] *The milestone "Acceptance of IEG-C security accreditation package" will be achieved when NSAB approval is granted at EDC+13mo.*

[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.*

3.8. System Integration Testing (SIT) + System Acceptance Testing (SAT) + User Acceptance Testing (UAT)

[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 SHALL achieve Purchaser approval of the associated documentation.*

3.9. Deployment Authorization (DA)

3.9.1. Successful completion of RFC process is a prerequisite for adding the IEG-C to the AFPL, which is a pre-requisite for authorization to deploy the IEG-C on to NATO networks.

[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-61] *The Contractor SHALL have handled any change to satisfy the security requirements.*

[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-63] *The Contractor SHALL have completed and 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-64] *The Contractor SHALL have completed the Site Acceptance Plan and have received the approval by the Purchaser.*

[SOW-65] *The Contractor SHALL have completed the Site Acceptance Test Cases and have received the approval by the Purchaser.*

[SOW-66] *The Contractor SHALL have completed the Operational System Acceptance (OSA) Plan and have received the approval by the Purchaser.*

[SOW-67] *The Contractor SHALL have completed the OSA Test Cases and have received the approval by the Purchaser*

[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.*

3.9.2. The achievement of DA is subject to the Purchaser approval which is based on accomplishment of the criteria listed in Table 9 The DA Success Criteria

[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.*

Serial	Requirement
1.	The IEG-C is added to the AFPL
2.	The IEG-C has obtained CAB approval
3.	Training for operators is completed
4.	High-level design of Information Entities is completed.
5.	Security Accreditation Documentation is approved by the Security Accreditation Authority
6.	The Site Acceptance Plan is approved by the Purchaser
7.	Site Acceptance Test Cases are approved by the Purchaser
8.	Operational System Acceptance (OSA) Plan are approved by the Purchaser
9.	OSA Test Cases are approved by the Purchaser

Table 9 The DA Success Criteria

3.10. Provisional System Acceptance (PSA)

3.10.1. The IEG-C will be considered as having achieved the PSA (EDC+20mo) milestone when all the relevant system prerequisites have been completed successfully and the first operational IEG-C Gateway is activated.

3.10.2. The criteria for achieving PSA are listed below:

[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 169) 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-71] *The Contractor SHALL have delivered all functionalities of IEG-C defined within Work Packages Scope (Annex B2)*

[SOW-72] *The Contractor SHALL have trained all required personnel according to Section 6.6: Training.*

[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-74] *The Contractor SHALL have satisfied the security requirements (see Section 10: Security).*

[SOW-75] *The Contractor SHALL have migrated on IEG-C all services required to support the information exchange requirements for the CIS interconnection.*

[SOW-76] *The Contractor SHALL ensure all performance and availability requirements specified in this SOW (Annex A, SRS) have been met.*

[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-78] *The Contractor SHALL have supplied the spare parts and consumables.*

[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-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-81] *The Contractor SHALL have provided the Configuration Management database (CMDB) in a format that is compatible with the Purchaser CMDB tools.*

[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-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.*

3.10.3. It is important to note that PSA is not only dependent on compliance against testable requirements, but will require non-testable requirements to be met too.

[SOW-84] *The Contractor SHALL handle all observations and deficiencies from the Formal Test Phases following the Defect Management Process and SHALL satisfactory resolve them before awarding PSA.*

3.10.4. The Contractor SHALL have completed and received 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 PSA Site (SHAPE).First Site Acceptance

[SOW-85] *In addition to the requirements set below, the Contractor SHALL achieve, for the Mons site, the requirements as set below in 3.12 Site Acceptance and SECTION 10: Security Accreditation.*

3.10.5. The achievement of PSA is subject to the Purchaser approval which is based on accomplishment of the criteria listed in Table 10 PSA success criteria.

[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.*

Serial	Requirement
1.	The IEG-C documentation is delivered and approved
2.	The IEG-C functionalities are delivered
3.	The IEG-C Training is completed
4.	Spare parts and consumables are delivered
5.	All IEG-C software components (including ITSM tools) are on the AFPL (Approved Fielded Product List)
6.	PBL and OBL are updated and the corresponding CMDB data provided to the Customer
7.	PCA and FCA reports are delivered and corrective actions completed

8.	Site Security Accreditation is approved by the Security Accreditation Authority
9.	The IEG-C is integrated with Core Services, Service Management and Monitoring
10.	IEG-C Services are migrated from the old IEG-C prototype in SHAPE to the new IEG-C-02
11.	Performance and Availability requirements set in Annex A of this SOW (SRS) are met
12.	The IEG-C-02 is installed, tested and activated

Table 10: PSA success criteria

3.11. Site Accreditation

Site accreditation is addressed in Section 10 and will apply to each site individually.

3.12. Site Acceptance

3.12.1. The following requirements will apply to each of the locations that will host an IEG-C.

3.12.2. The completion of acceptance all locations will mean the completion of the Site Acceptance milestone.

[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-88] *The Contractor SHALL meet all the PSA-related requirements.*

[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-90] *The Contractor SHALL have installed, tested and activated the IEG-C(s) at the site.*

[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-92] *All performance and availability requirements specified in this SOW SHALL have been met by the Contractor.*

[SOW-93] *The Contractor SHALL train all required personnel according to Section 6.6: Training.*

[SOW-94] *The Contractor SHALL have supplied the spare parts and consumables.*

[SOW-95] *The Support Services SHALL have been updated as required.*

[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-97] *The Contractor SHALL have provided the Operational Baseline (OBL) as described in SECTION 12: Configuration Management to reflect the actual Site configuration.*

[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.*

3.12.3. The SAA has issued the Statement of Accreditation for the interconnection via IEG-C at the site.

3.12.4. Site Activation Meetings

The achievement of Site Activation is subject to the Purchaser approval, in writing. Site Activation will be established at a meeting convened between the Contractor and the Purchaser for that purpose. At that meeting the Contractor will present to the Purchaser evidence that all conditions for Site Activation as described in Section 3.12 Site Acceptance and summarized in Table 11: Site Activation Criteria have been met.

Serial	Requirement
1.	PSA requirements are met
2.	The IEG-C gateways for the site are installed, tested and activated as per ILS and TVV requirements
3.	All deliverables are delivered
4.	All IEG-C Services are migrated
5.	Performance and Availability requirements set in Annex A of this SOW (SRS) are met
6.	The IEG-C Training is completed
7.	Spare parts and consumables for the site are delivered
8.	PBL and OBL are updated and the corresponding CMDB data provided to the Customer
9.	Site Security Accreditation is approved by the Security Accreditation Authority

Table 11: Site Activation Criteria

3.13. Operational Test and Evaluation (OT&E)

[SOW-99] *The Contractor SHALL conduct OT&E as defined in Sections SECTION 7 and SECTION 8.*

[SOW-100] *The Contractor SHALL have successfully implemented or achieved the Operational Acceptance Criteria (OAC) that apply to this SOW and have been included in Annex A (SRS).*

[SOW-101] *The Contractor SHALL note that the achievement of the OT&E milestone is subject to the Purchaser acceptance.*

3.14. Final System Acceptance (FSA)

3.14.1. FSA (EDC+27mo) is the act by which the Purchaser has evaluated and determined that the implemented IEG-C System meets the requirements of the Contract, and that the Contractor has fully delivered all requirements.

[SOW-102] *The Contractor SHALL meet all PSA milestone requirements (see par.3.10) as well as Site Activation milestone requirements (see par.3.12: Site Acceptance) for all the sites to be implemented under this contract.*

[SOW-103] *The Contractor SHALL execute all implementation activities according to SECTION 3 at all the sites to be implemented under this contract.*

[SOW-104] *The Contractor SHALL install the most recent version of implemented IEG-C.*

[SOW-105] *The Contractor SHALL fully implement the centralised management and control of the IEG-C according to the requirements specified in this SOW.*

[SOW-106] *The Contractor SHALL deliver a complete and updated set of documents (e.g. Functional Baseline, Product baseline, Operational baseline)*

[SOW-107] *The Contractor SHALL have provided the Configuration Management database (CMDB) in a format that is compatible with the Purchaser CMDB tools.*

[SOW-108] *The Contractor SHALL activate Support Services at all the FSA Sites.*

[SOW-109] *The Contractor SHALL have executed all agreed test cases, and all tests SHALL have a status "PASS".*

[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.*

3.14.2. The SAA has issued the Statements of Accreditation for the **IEG-C** at all the Sites.

[SOW-111] *The Contractor SHALL deliver all deliverables (SECTION 15), and conducted all activities, as specified in this Contract.*

[SOW-112] *The Contractor SHALL close to the satisfaction of the Purchaser all outstanding issues, failures, and deficiencies.*

3.14.3. Site FSA Meetings and Success Criteria

The achievement of FSA (EDC+27mo) is subject to Purchaser approval, in writing. Project FSA will be established at a meeting convened between the Contractor and the Purchaser for that purpose. At that meeting the Contractor shall present to the Purchaser evidence that all conditions for FSA, as described in 3.14.1 and summarized in Table 11 FSA Success Criteria, have been met.

[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.*

Serial	Requirement
1.	PSA and OT&E milestones are achieved
2.	All the IEG-Cs in the scope of this SOW and listed in ANNEX B Implementation Scope are delivered and are operational
3.	All changes to IEG-C software components (including ITSM tools) are on the AFPL (Approved Fielded Product List)
4.	All site have the latest version of IEG-C system solution
5.	FBL, PBL and OBL are updated and the corresponding CMDB data provided to the Customer
6.	Site Security Accreditation for all FSA sites is approved by the Security Accreditation Authority
7.	IEG-C Services are migrated from the old IEG-C prototypes to the new IEG-C
8.	Performance and Availability requirements set in Annex A of this SOW (SRS) are met
9.	Test and Acceptance phases with Test Reports are provided to the Customer
10.	Legacy Gateways (WP3 and WP4 locations) have been decommissioned and removed

Table 12: FSA Success Criteria