NATO Communications and Information Agency

List of Requirements

NATO BALLISTIC MISSILE DEFENCE (BMD)
SYSTEMS ENGINEERING, INTEGRATION & TEST

IFB-CO-14974-BMD

Annex A to the Statement of Work

See separate document

IFB-CO-14974-BMD-Book II-Part IV-SOW-Annex A - List of Requirements

ANNEX B – TVV Definitions

The purpose of this Annex is to provide definitions of the terms used in for the Test, verification, Validation activities define din Test and acceptance section of this SOW.

B.1. TEST DEFECT CATEGORIZATION

Category	Definition
Severity	The severity of a failure is the degree of impact that the failure has on the development or operation of a component or system or user function. The severity of the failure SHALL initially be proposed by the tester but SHALL officially be set in agreement with all the stakeholders. When agreement cannot be reached the Purchaser's PM will set the severity.
Priority	The priority of a defect defines the order in which defects SHALL be resolved. The priority of the defect SHALL initially be proposed by the tester but SHALL officially be set in agreement with all the stakeholders. When agreement cannot be reached the Purchase's PM will set the priority.

Table 1: Definitions for Defect Categorization

B.1.1. Severity

Critical	• Functional failure that inhibits users from accomplishing a primary task (Functional) • Failure of critical user requirements • Inability to install system software in accordance with provided documentation (Portability/Documentation) • Occurrence of a transient error and/or infinite loops/system hanging (Reliability) • System/application crashes on major functions or unsuccessful recovery (Functional or Reliability) • Loss of data, inconsistent results (database/data integrity problems) or corruption of database (Reliability) • Inaccurate result or calculation of essential function (Usability) • Poor reliability or performance which may degrade the overall operation/functioning of the system (Performance Efficiency) • Slow response time of an essential user function (user identified) that degrade the user operation.

	• Failure of a Security function or cause of security violation (Security) • Failure of exchange of information/data with its affiliates or with its shared environment (Compatibility)
Major	• Failure of a function or defect that impacts the normal system operation but an user acceptable workaround exists (Functional) • Absence of or incorrect validity checks in accordance with user specification or as expected by the software (Reliability) • Display of a misleading information resulting in confusing or incorrect processing (Usability) • Slow response time of common user functions (Performance Efficiency) • Editing the same field/record/data concurrently causing database integrity problems (Reliability)
Minor	• Failure of a non-essential function that does not impact the normal operational use of the application (Functional) • Defects that does not impact the overall quality of the software
Cosmetic	• The failure is related to the enhancement of the system where the changes are related to the look and feel of the application, and not part of the usability requirements of the system. (Usability)

Table 2: Classification of defects based on severity

B.1.2. Priority

Priority Class	Description
Urgent	The defect SHALL be resolved as soon as possible.
Medium	The defect SHALL be resolved in the normal course of development activities. It can wait until a new build or version is created.
Low	The defect is an irritant which should be repaired, but repair can be deferred until after more serious defects have been fixed.

Table 3: Priority Classes for Defect Classification

B.2. VERIFICATION METHODS

Demonstration

Technique used to demonstrate correct operation of the submitted element against operational and observable characteristics **without using physical measurements** (no or minimal instrumentation or test equipment).

Demonstration is sometimes called 'field testing'.

It generally consists of a set of tests selected by the supplier to show that the element response to stimuli is suitable or to show that operators can perform their assigned tasks when using the element.

Observations are made and compared with predetermined/expected responses. Demonstration may be appropriate when requirements or specification are given in statistical terms (e.g. meant time to repair, average power consumption, etc.).

Test

Technique performed onto the submitted element by which functional, measurable characteristics, operability, supportability, or performance capability is **quantitatively verified when subjected to controlled conditions** that are real or simulated.

Testing often uses special test equipment or instrumentation to obtain accurate quantitative data to be analysed

Inspection:

Technique based on **visual or dimensional examination** of an element.

The verification relies on the human senses or uses simple methods of measurement and handling.

Inspection is generally non-destructive, and typically includes the use of sight, hearing, smell, touch, and taste, simple physical manipulation, mechanical and electrical gauging, and measurement.

No stimuli (tests) are necessary.

The technique is used to check properties or characteristics best determined by observation (e.g. - paint colour, weight, documentation, listing of code, etc.).

Analysis

Technique based on **analytical evidence obtained without any intervention on the submitted element** using mathematical or probabilistic calculation, logical reasoning (including the theory of predicates), modelling and/or simulation under defined conditions to show theoretical compliance.

Mainly used where testing to realistic conditions cannot be achieved or is not cost-effective

ANNEX C

PURCHASED FURNISHED ITEMS (PFI)

The PFI List is as follows:

PFI Name	Description	Date
Project Website (NR Web Portal)	Portal to exchange project documentation up to NR	EDC + 2 Weeks
Test Bed Facility	Integration testbed facilities for integration testing of the ITB component at its premises in The Hague, Netherlands.	During ITB OFS Test Events
Office space during test execution	Office desk, internet connection for two people	During ITB OFS Test Events
NATO BMC3I Systems	a. ACCS b. AirC2IS c. CBRN FS d. ETEE e. NCOP f. Intel FS g. TOPFAS	During ITB OFS Test Events
Legacy Systems	a. ICC/LSID b. NIRIS c. CSI d. Engility JRE Hub e. TDACS	During ITB OFS Test Events
Comms. Legacy Applications	The followings are simulation communication application which are mandated by the Nations for exchanging simulation data with ITB. a. Remote Site Manager (US) b. UvT (DEU) The following is communication legacy application offered as option	During ITB OFS Test Events

	by the Program to Nations for supporting to exchange of simulation data: c. NCIA BMGW	
National C2 Systems	SAMOC	During ITB OFS Test Events
National Constructive Simulations	National sensors / Sea-based and Land-based weapons a. EADSIM b. JROADS	During ITB OFS Test Events
NATO Core Services	a. Chat b. VoIP	During ITB OFS Test Events
Map Server including Map Data	Map Server	During ITB OFS Test Events
Communication Network Infrastructure	Network Infrastructure for separate secure networks with configuration information	During ITB OFS Test Events
Hosting infrastructure	To support development including servers, security services for servers, workstations, and wide area network connections.	4 Weeks before SAT
ITB Existing Documentation	Access to ITB Documentation at Purchaser facilities	EDC + 2 weeks
ITB Existing System	Access to ITB System at Purchaser facilities	EDC + 2 weeks
Training Facility	To support training, the Purchaser will provide the following basic facilities: room, power supply, tables, chairs, network connectivity necessary to perform the trainings courses in the Purchaser's facilities.	During Training

Table 1 PFI

ANNEX D – PERSONNEL QUALIFICATION

Please use template in Book I Annex G to provide qualification for the personnel.

1.1 Project Manager

SOW-1. The Contractor shall designate a Project Manager (PM), who will direct and co-ordinate the activities of the Contractor's project team.

SOW-2. The Project Manager shall be the Contractor's primary contact for the Purchaser's Project Manager and shall conduct all major project design, test, and status reviews.

SOW-3. The Project Manager shall be prepared at all times to present and discuss the status of Contract activities with the Purchaser's Project Manager, Contracting Officer, or Technical Director.

SOW-4. The Project manager shall be responsible for performance and completion of tasks and delivery orders; for establishing and monitoring project plans and schedules. The Project Manager shall have full authority to allocate resources to insure that the established and agreed upon plans and schedules are met. He shall manage costs, technical work, project risks, quality, and corporate performance. He shall manage the development of designs and prototypes, test and acceptance criteria, and implementation plans. He shall establish and maintains contact with Purchaser, Subcontractors, and project team members. He shall provide administrative oversight, handle contractual matters and serve as a liaison between the Purchaser and corporate management. He shall ensure that all activities conform to the terms and conditions of the Contract and Work Package procedures.

SOW-5. The Project Manager shall meet the following qualifications:

a. Education: Master's degree with in management, engineering, or business administration. Formal certification through Project Management Institute or equivalent source, PRINCE 2 certified or equivalent (e.g. PMP).

b. Experience: At least seven years in project management in the area of software development projects.

1.2 Technical Lead

SOW-6. The Contractor shall designate a Technical Lead for the project.

SOW-7. The Technical Lead shall lead the analysis, design, development, integration, and follow-on enhancement efforts of the Contractor.

SOW-8. The Technical Lead shall plan and co-ordinate project management and engineering. He shall provide comprehensive definition of all aspects of system development from analysis of mission needs to verification of the overall ITB 6 OFS system performance. He shall be competent in technical disciplines as applied to government and commercial information and communications systems. He shall supervise the work of a design, development, integration, test, and implementation team. He shall prepare trade-off studies and evaluations for vendor equipment. He shall recommend design changes/enhancements for improved system performance.

SOW-9. The Technical Lead shall meet the following qualifications:

a. Education: Master's degree in engineering or computer science.

b. Experience: At least seven years in system design and integration, especially on DIS, HLA and distributed simulation systems. At least five years in the design, integration, or implementation of information systems. At least 2 years experienced on C2 and BMD areas including interoperability concept. At least 2 years' experience on virtualization. Knowledgeable on interoperability standards (Link-16, JREAP, Adat-P3/APP-6, SIMPLE).

1.3 Test Director

SOW-10. The Contractor shall designate a Test Director for all test activities conducted under this Contract.

SOW-11. The Test Director shall direct test planning, design and tools selection. He shall establish guidelines for test procedures and reports, co-ordinate with Purchaser on test support requirements and manages Contractor test resources.

SOW-12. The Test Director shall meet the following qualifications:

a. Education: Bachelor's degree in engineering. At least Foundation level ISTQB certification (or equivalent)

b. Experience: At least seven years in the design and execution of information systems tests.

1.4 Field Engineer

SOW-13. The Contractor shall designate a Field Engineer (FE) to conduct site surveys, prepares implementation plans, prepares implementation procedures, supervises installation and activation, reports on installation status, manages repair and modifications to systems/equipment, performs field maintenance, and performs system configuration changes based upon approved specifications, as the ITB Build 6 system administrator of ITB 6 OFS.

a. Education: Bachelor's degree on IT or similar universities.

b. Experience: At least five years in the installation and support of information systems. At least 5 years' experience on distributed interactive simulation (DIS) applications and high level architecture (HLA) standard. Experienced on maintenance of security posture for labs and application. Hands on experience on virtualization, network protocols, Windows and LINUX.

SOW-14. The FE designated as the ITB Build 6 System Administrator shall possess a valid Security clearance to the level of NATO Cosmic Top Secret (CTS).

1.5 ILS Engineer

SOW-15. The Contractor shall designate an ILS Engineer to create and help execute plans for the integrated logistics support (ILS), analyse adequacy and effectiveness of current and proposed logistics support provisions and supervise the efforts of other logistics personnel in the execution of assigned tasks. He/she provides subject matter expertise in the areas of Service Design, Service Transition, and Service Operation as introduced by the Information Technology Infrastructure Library (ITIL) or equivalent best practices and Software Life Cycle Support and Maintenance.

a. Education: Bachelor's degree

b. Experience: At least five years in the ILS area in support of NATO's project or a NATO nation's project. At least three years in the development of logistics doctrine; operational concepts, support concepts, and maintenance concepts; ILS requirements; tactics, techniques and procedures; standard operating procedures and other support documentation, ITIL discipline and Life Cycle Support Maintenance.

1.6 Configuration Manager

SOW-16. The Contractor shall designate a Configuration Manager for all configuration activities conducted under this Contract.

SOW-17. The Configuration Manager shall maintain a process for tracking the life cycle development of system design, integration, test, training, and support efforts. He shall maintain continuity of products while ensuring conformity to Purchaser requirements and commercial standards. He shall maintain configuration control records and databases.

SOW-18. The Configuration Manager shall meet the following qualifications:

a. Education: Associate's degree or two years of technical training.

b. Experience: At least three years in technical system and software configuration management. At least two years in computer and communication systems development, including physical and functional audits and software evaluation, testing and integration.

1.7 Quality Assurance Manager

SOW-19. The Contractor shall designate a qualified individual to serve as the Quality Assurance Manager for activities under this Contract.

SOW-20. The Quality Assurance Manager shall report to a separate manager within the Contractor's organisation at a level equivalent to or higher than the Project Manager.

SOW-21. The Quality Assurance Manager shall establish and maintain process for evaluating software, hardware, and associated documentation. He shall determine the resources required for quality control. He shall maintain the level of quality throughout the system life cycle. He shall develop project quality assurance plans and conduct formal and informal reviews at predetermined points throughout the system life cycle.

SOW-22. The Quality Assurance Manager shall meet the following qualifications:

a. Education: Bachelor's degree.

b. Experience: At least four years working with quality control methods and tools. At least four years supporting system and software development and test projects.

ANNEX E – Support and Maintenance Concept Definitions

Definition

[1] Level of Support: Level of support indicates a specific extent of technical assistance in the total range of assistance that is provided by an information technology product to its customer. The Service management is divided in three different level of service, which interface each other, in order to activate the proper level of maintenance in accordance with the event (incident) happened on the system.

[2] Level of Maintenance: are various echelons at which maintenance tasks are performed on systems and equipment. The levels are distinguished by the relative sophistication of skills, facilities and equipment available at them. Thus, although typically associated with specific organisations and/or geographic locations, in their purest form, the individual maintenance levels denote differences in inherent complexity of maintenance capability.

Support Concept

[3] The Support concept is the set of activities and processes in charge of managing the various level of maintenance and to escalate the problem to the appropriate level in accordance with the defined responsibilities.

[4] It uses a systematic approach, to minimise the logistic delay and assure the maximum level of Service and Operation availability.

[5] It is based on the Incident management process defined in ISO/IEC 20000 and ITIL framework or equivalent.

[6] The objective of Incident Management is to restore normal operations as quickly as possible with the least possible impact on either the business or the user, at a cost-effective price

First Level Support Process

[7] The 1st Level Support Process implements the Incident Management process in accordance with the ISO/IEC 20000 and ITIL framework or equivalent;

[8] As part of the Incident Management, the Service Desk receives the issue from the user, puts it into a standard format (Trouble Ticket (TT)), performs an initial assessment and distributes it to the predefined actors to solve it

Second Level Support Process

[9] The 2nd Level Support Process implements the Problem Management process in accordance with the ISO/IEC 20000 and ITIL framework or equivalent;

[10] The Problem Management process receives the TT from the Service Desk and performs the following tasks (not limited to):

a. (Re-)evaluation of TT category, criticality and priority,

b. Identification of the root cause of the issue (e.g. by issue replication testing),

c. Identification of workarounds,

d. Identification and initial planning of possible short, medium and long-term solutions (e.g. workarounds, patches, or new baseline or CI releases),

e. Create Problem Analysis Report and Change Request incl. schedule of implementation, and synchronisation with the Baseline Maintenance process;

f. Presentation of the Problem Analysis Report and Change Request in accordance with the configuration management processes,

g. Monitor and Control the approved Change Request during implementation,

h. Trigger 3rd Level Support and/or 3rd Level Maintenance process to implement the Change Request, in case the incident cannot be solved at 2nd level;

i. Perform the post- Change Request implementation review.

Third Level Support Process

[11] The 3rd Level Support Process implements the Deployment and Release Management process in accordance with the ISO/IEC 20000 and ITIL framework or equivalent.

[12] It Includes the Maintenance Process as part of the Release Management

[13] The Deployment and Release Management process receives the approved Change Request from the 2nd Level Support and performs the following tasks (not limited to):

a. activating Level 3 maintenance when new solutions shall be developed;
a. development of the solution (e.g. new CI Fix, Repair, Replacement, Patch, or Release);
b. testing of the solution (e.g. Regression testing, issue/deficiency replication testing);
c. update of baseline content and status;
d. release of the solution (release unit/record);
e. delivery and deployment of the solution.

Maintenance Concept

[14] The Maintenance Process need to ensure the maintainability of the PBL and the OBL. The Baseline Maintenance Process implements modifications to be made either proactively or reactively to the PBL to correct faults and/or deficiencies, to improve performance or other PBL attributes, or adapt the PBL/OBL to a modified environment.

[15] The maintenance concept includes the following activities:

a. the Maintenance of all the Configuration Items and all related items,
b. the execution of all the required preventive and corrective maintenance activities for all the system and its subsystems for each level,
c. the allocation of the Maintenance tasks to the respective maintenance levels and the related organisation

[16] The Maintenance Concept is the set of activities and processes in charge of restoring the system functionality in the shortest time possible.

[17] The Baseline Maintenance process is decomposed into 1st, 2nd, 3rd and 4th Level Maintenance tasks.

First Level of Maintenance

[18] It is responsible for the very basic maintenance activities. It is responsible to activate the second level of maintenance when it is needed.

[19] It implements the initial preventive Maintenance procedures and any additional Service/Capability and/or site specific procedures that are defined in the corresponding O&M Manual. All 1st Level Maintenance procedures do not require specialised tools and/or specialised personnel.

Second Level of Maintenance

[20] It is responsible of isolation and resolution of system-level maintenance and management of deficiency reports and repair. It is responsible to activate the third level of maintenance when it is needed.

[21] It implements the initial preventive Maintenance procedures and any additional Service/Capability and/or site specific procedures that are defined in the corresponding Manual. All 2nd Level Maintenance procedures do not require specialised tools and/or specialised personnel.

Third Level of Maintenance

[22] It is responsible of any support that involves a change to the system baseline, such as software patches or new releases. It is responsible of specialised hardware repair, if requested.

[23] Third level maintenance is activated by third level support and can be initiated either to define the solution to a problem (corrective maintenance) or to maintain up to date software configuration e.g. due to security patches, operating system obsolescence and upgrades, minor software configuration changes due to operational/interface needs (adaptive maintenance following changes to the underpinning hardware, firmware and software environment).

[24] It implement the initial preventive Maintenance procedures and any additional Service/Capability and/or site specific procedures that are defined in the corresponding Manual. 3rd Level Maintenance procedures can require specialised tools and/or Personnel

Fourth Level of Maintenance

[25] It is the responsibility of the hardware vendor or the software original developer. It is activated from the 3rd level of maintenance only when is needed.

[26] It is responsible for Software(SW)/Firmware(FW) debugging, re-coding and testing (both in simulated and emulated environments), SW/FW patch creation and deployment, configuration and change management. The tasks should be performed by software engineers/developers in properly configured environments (SW development and testing facilities) under configuration control.

NATO Communications and Information Agency

Common Documents
Project Security Instructions

NATO BALLISTIC MISSILE DEFENCE (BMD)
SYSTEMS ENGINEERING, INTEGRATION & TEST

CO-14974-BMD

Annex F to the Statement of Work

This Page Intentionally Left Blank.

REVISION SHEET

ECP No	Revision	Date
Initial Release	-	05.09.2019

This Page Intentionally Left Blank

TABLE OF CONTENTS

LIST OF TABLES AND FIGURES

This Page Intentionally Left Blank

1. INTRODUCTION

1.1 Purpose

(1) This document contains the Project Security Instructions (PSIs) for the CO-14974-BMD and is issued pursuant to NATO Security Policy (Reference A) published by the NATO Security Committee and its supporting directives as described in Reference B and in particular the directive of Reference and C of Reference D.

(2) It describes the Contractor's obligations to protect NATO classified information against related security threats (i.e. espionage, compromise, or unauthorised disclosure) and provides specific security rules, regulations and procedures, which shall be applied by the Contractor addressing the minimum security requirements for the protection of NATO classified information received or produced under the Contract.

(3) This document forms part of the Contract and provides direction to ensure compliance by Contractor on the protection of NATO classified information.

(4) This document describes the security requirements for Article 28 of Part 2 of the Contract.

(5) The PSIs are to be reviewed regularly and amended as necessary in consultation with the NATO Office of Security (NOS), the Air and Missile Defence Security Accreditation Board (ASAB) and National Security Authorities/Designated Security Authorities (NSAs/DSAs) so that any sensitivities relating to the Contract are identified and managed to ensure that the most appropriate degree of security is afforded throughout the Contract.

(6) The NSAs/DSAs/ Security Accreditation Authority (SAAs) are responsible for the implementation and oversight of security for NATO classified information entrusted to their Contractors. For NATO, NOS is the primary security accreditation authority, however, for NATO sites within Allied Command Operations (ACO) area of responsibility, this authority is delegated to SHAPE J2. For these sites Reference Q and Reference R are applicable, which may have more stringent control measures than the top-level NATO Security Directives.

1.2 References

(7) The references for these PSIs are listed below:

A. NATO Security Policy - C-M(2002)49-COR12, 14-Sep-15

B. "Roadmap" to NATO Security Policy, Supporting Directives, Supporting Documents and Guidance Documents - Version 2.14, 18-Oct-19

C. Directive on Classified Project and Industrial Security - AC/35-D/2003-REV5, 13 May 15

D. Technical and Implementation Directive on Supply Chain Security for COTS CIS Security Enforcing Products - AC/322-D(2017)0016 (INV), 30-Mar-17

E. ASAB Terms Of Reference (TOR) - AC/336(AIRC2)N(2019)0014-AS1 (INV), 26-Sep-19

F. Air Command & Control (AirC2) Security Accreditation Board (ASAB) Security Accreditation Strategy (ASAS) - NCIA/AIRC2POS/2017/00704, Version 1.0, 10-May-17

G. Directive on the Security of Information - AC/35-D/2002-REV4, 17-Jan-12

H. Directive on Personnel Security - AC/35-D/2000-REV7, 07-Jan-13

I. ACCS Community Security Requirement Statement (CSRS) - Version 2.1, 29-Apr-19

NGCS CSRS – Version 2, June 19

J. INFOSEC Technical & Implementation Directive for the Interconnection of Communication and Information Systems (CIS) - AC/322-D/0030-REV5, 23-Feb-11

K. Supporting Document on the Interconnection of NATO RESTRICTED CIS to the Internet - AC/322-D(2010)0058, 21-Dec-10

L. Technical & Implementation Directive for CIS Security - AC/322-D/0048-REV3, 18-Nov-19

M. Security Operating Procedures (SecOPs) for End-users of NATO RESTRICTED Automated Information System (NR AIS) – SECOPS_NR_AIS.2.0 (NCIARECCEN-4-153089), 11-Jun-18

N. Security Classification for Fixed Positioned Air Defence Radar and Deployable Air Defence Radar - Revision B - SH/OPI/J3/AC2PM/SYS/18/006-320010, 08-Feb-18

O. NATO Guidance on ACCS IP Addresses - Classification & Distribution - NCIA/AMDC2/2018/0037, Version 1.0, 2015

P. Security Classification Guidelines for ACCS Artefacts - NCIA/AMDC2/2018/00377, Version 2.0, 04-Nov-15

Q. (NU) ACO Security Directive – AD 070-001, Jan 2019

R. (NR) ACO Communication and Information System (CIS) Security – AD 070-005, Jan 2019

S. (NU) NATO BMD Security Classification Guide - BMD-PO-PRG-SCG-108-2.0, 30-Sep-20

1.3 Authority

(1) Requests for clarification or recommended changes or revisions to this PSI shall be directed to NCIA Security Officer (NCIA SO), who will co-ordinate as appropriate with the relevant authorities. Changes will not be made without notification and approval of NOS/Air and Missile Defence Security Accreditation Board (ASAB) (Reference E and Reference F).

1.4 Definitions

(1) The applicable abbreviations and definitions of frequently used terms are listed in Table 1:

Access	The ability and opportunity to obtain knowledge of classified information
NCIA SO	A nominated NCIA CIS Security Officer from the Purchaser responsible for the overall security activities for this project. For this contract, this will be performed by Head CIS Security AMDC2
AIS	Automatic Information System
AfT	Approval for Testing
Attestation of Personnel Security Clearance (APSC)	An approved format to confirm the security clearance level of an individual in the context of a contract involving NATO classified information.
Breach of Security	An act or omission, deliberate or accidental, contrary to NATO Security Policy and supporting directives, that results in the actual or possible compromise of NATO classified information or supporting services and resources (including, for example, classified information lost while being transported; classified information left in an unsecured area, where persons without an appropriate PSC have unescorted access; an accountable document cannot be found; classified information has been subjected to unauthorised modification; destroyed in an unauthorised manner or, for CIS, there is a denial of service).
CIS	Communication Information System. An assembly of computer hardware, software, and firmware configured for the purpose of automating the functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating, or otherwise manipulating data, information, and textual material.
CIS Security	The application of security measures for the protection of communication, information and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation.

Classified Information	Any information (namely, knowledge that can be communicated in any form) or material determined to require protection against unauthorised disclosure and which has been so designated by a security classification.
Classified Meeting	A conference, seminar, symposium, exhibition, convention, or other gathering that is conducted by a participant or by a cleared Contractor during which classified information is disclosed.
Commercial Courier Company	Commercial company that offers a service where a consignment is moved under a trace and tracking scheme.
Compromise	Compromise denotes a situation when - due to a breach of security or adverse activity (such as espionage, acts of terrorism, sabotage or theft) - NATO classified information has lost its confidentiality, integrity or availability, or supporting services and resources have lost their integrity or availability. This includes loss, disclosure to unauthorised individuals (e.g. through espionage or to the media) unauthorised modification, destruction in an unauthorised manner, or denial of service.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals or entities.
Contract	A legally enforceable agreement to provide goods or services.
Contractor	An industrial, commercial or other entity that seeks or agrees to provide goods or services.
Courier	A person officially assigned to hand-carry material.
Document	Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, photographs, paintings, drawings, engravings, sketches, working notes and papers, carbon copies or ink ribbons, or reproductions by any means or process, and sound, voice, magnetic or electronic or optical or video recordings in any form, and portable IT equipment with resident computer storage media, and removable computer storage media.
DSA	Delegated Security Authority. In certain circumstances the National Security Authority (NSA) may formally delegate its responsibilities to a subordinated entity. When this formal delegation has taken place the entity will become a Delegated Security Authority (DSA).
Facility Security Clearance (FSC)	An FSC is an administrative determination by which an NSA/DSA formally recognises the capacity and reliability of Contractor's facilities to manage generate and have access to NATO classified information up to a certain level.
Infraction	A security infraction is an act or omission, deliberate or accidental; contrary to NATO Security Policy and supporting directives that does not result in the actual or possible compromise of NATO classified information. (E.g. classified information left unsecured inside a secure facility where all persons are appropriately cleared, failure to double wrap classified information, etc.).
Information	Any information provided to, generated in, or used in the Contract. This information may be of any form or type. (I. e including scientific, technical, business, or financial data, and includes photographs, reports, manuals, threat data, experimental data, test data, designs, computer software, specifications, processes, techniques, inventions, drawings, technical writings, sound recordings, pictorial representations, and other graphic presentations). Data also includes magnetic tape, computer memory, or any other forms and whether or not subject to copyright, patent, or other legal protection.
IVCP	International Visit Control Procedures

NATO Classified Information	Means information or material determined by or on behalf of NATO to require protection against unauthorised disclosure which has been so designated by a security classification NR or above.
NATO RAP	NATO Recognised Air Picture
Need-to-know	The principle according to which a positive determination is made that a prospective recipient has a requirement for access to, knowledge of, or possession of information in order to perform official tasks or services .
National Security Authority (NSA)	An authority of a NATO nation which is responsible for the maintenance of security of NATO classified information in national agencies and elements, military or civil, at home or abroad.
Personnel Security Clearance (PSC)	A determination that an individual is eligible to have access to classified information.
Personnel Security Clearance Certificate (PSCC)	An approved format used by NSAs/DSAs to confirm the level and validity of a PSC.
Project Security Classification Guide (PSCG)	Part of the program (project) security instructions (PSI) which identifies the elements of the program that are classified, specifying the security classification levels. The security classification guide may be expanded throughout the program life cycle, and the elements of information may be re-classified or downgraded.
Risk	The likelihood of a vulnerability being successfully exploited by a threat, leading to a compromise of confidentiality, integrity and/or availability and damage being sustained.
Subcontractor	Any agreement, contract, subcontract or purchase order made by the Contractor with any other party in order to fulfil any part of this Contract. A contractor to whom a prime Contractor lets a sub-contract.
Threat	The potential for compromise, loss or theft of NATO classified information or supporting services and resources. A threat may be defined by its source, motivation or result, it may be deliberate or accidental, violent or surreptitious, external or internal.
Vulnerability	A weakness, an attribute, or lack of control that would allow or facilitate a threat actuation against NATO classified information or supporting services and resources.

Table 1 - Definitions

2. SECURITY INSTRUCTIONS

2.1 Records of Employees

(1) The Contractor shall maintain a record of his employees taking the project and who have been cleared for access to NATO classified information. This record must show the period of validity and the level of the clearances.

2.2 Security Classifications and Markings

(1) Security classifications used for the Contract shall indicate the sensitivity of NATO information and are applied in order to alert recipient to the need to ensure protection, in accordance with Reference G, in proportion to the degree of the damage that would occur from unauthorised access or disclosure. The security classifications shall be applied only to those aspects of a contract that must be protected, and the level of such classifications must be strictly related to the degree of protection required.

(2) The word “NATO” is a qualifying marking which signifies that the document is the property of NATO even if the containing information remains the property of the owner. The originator of the information is responsible for determining the security classification and initial dissemination of information (see Appendix 2). The classification level of NATO information shall not be changed, downgraded or declassified without the consent of the NCI Agency as the Contracting Authority.

(3) The following principles apply to the marking of NATO information for the Contract:

a. NATO SECRET (NS) – where unauthorised disclosure would result in grave damage to NATO;

b. NATO CONFIDENTIAL (NC) – where unauthorised disclosure would be damaging to NATO;

c. NATO RESTRICTED (NR) – where unauthorised disclosure would be detrimental to the interests or effectiveness of NATO.

d. NATO UNCLASSIFIED (NU) – where unauthorised access would be undesirable and shall be granted only based a “need-to-know” principle (e.g. internal used only) but does not required specific security protection. NU information is no considered as NATO classified information.

(4) The classification of a compilation of information from more than one source shall be co-ordinated among the sources to determine the appropriate NATO security classification. To assist in classifying information for this project, specific classification guidance is provided for this project in references N, O, P and S.

(5) The Contractor shall not change any level of security classification or de-classification of documentation or material, which may be carried out unless written authority in this respect is obtained from the Purchaser.

(6) The initial assessment that information should be classified, which was not previously identified for classification in a contract, may be made by the Contractor. In such case, the Contractor shall recommend to take appropriate classification action. However, the decision to classify information ultimately is the responsibility of the Contracting Authority or other designated classification authority.

(7) In the absence of clearly defined classification guidance, the Contractor may forward a classification proposal to the NCIA SO regarding interim classification, which when reviewed and approved may update the Contract Project Security Classification Guide (PSCG).

2.3 Personnel Security Clearances (PSCs)

(1) All Contractor/Subcontractor personnel handling NATO classified (e.g. NC/NS) information shall possess a valid Personnel Security Clearance (PSC) at the appropriate level defined based on the Reference A, Reference C, Reference H and defined in Reference I, have a “need-to-know” and shall be briefed on security procedures and their responsibilities by the nominated Facility

Security Officer acknowledging in writing that they fully understand their security responsibilities and the potential consequences if information passes into unauthorised hands either by intent or through negligence. A record of the acknowledgement of responsibilities by Contractor's employees shall be retained by the Contractor Security Officer.

(1) The Contractor shall deny access to NATO classified information to any persons other than those authorised to have access with appropriate PSC and determined by the "need-to-know" requirement.

2.4 Protection of NATO classified information

(1) All NATO classified information generated, held, used, or exchanged in connection with the Contract shall be stored, handled, safeguarded and transmitted in accordance with the NATO Security Policy as stated in C-M(2002)49 (Reference A) and all its supporting directives and guidelines, contract requirements and applicable national laws and regulations.

(2) The Contractor shall apply appropriate security mechanism and protection level for NATO information up to including NATO SECRET.

(3) If information classified at NATO CONFIDENTIAL or above is to be processed or stored at the Contractor premises, then a Facility Security Clearance must be in place in accordance with the provisions of the Directive on Classified Project and Industrial Security (Reference C).

2.4.1 Storage

(1) Storage of NATO classified Contract information and material is only permitted at sites for which an appropriate facility clearance in proportion to the security classification of such information and material has been issued by the responsible NSA/DSA.

(2) NATO SECRET and NATO CONFIDENTIAL Information shall not be left unattended or handled in a manner that could result in unauthorised access. It shall be stored in an approved safe or steel file cabinet that has an automatic locking mechanism and is afforded supplemental protection (NSA/DSA approved Intrusion Detection Systems or NSA/DSA approved Security Guard services) during non-working hours. When NATO SECRET and NATO CONFIDENTIAL information is not secured in a NSA/DSA approved container it may only be worked on in a restricted or closed area that prevents unauthorised personnel access to the information or material.

(3) NATO RESTRICTED information shall be stored in a manner that deters unauthorised access; for example, in a locked desk, cabinet or room to which access is controlled. When vacating an individual office at the close of normal working hours, the last person leaving is required to ensure that classified material is properly secured in the appropriate container(s), that the window(s) are fastened shut and that classified waste is also properly secured. Office security check sheets should be used as a reminder to office occupants of their responsibilities at the close of normal working hours..

(4) Unless specifically mandated by NSA/DSA or Contracting Authority, NR information is not required to be individually recorded or processed through a Registry System

2.4.2 Access

(1) Access to NATO UNCLASSIFIED Information shall be limited to individuals having a need-to-know. NATO UNCLASSIFIED Information does not require security protection. NATO UNCLASSIFIED Information may only be released to the general public (non-NATO nations, organisations, and individuals) when such release would not be against the interest of NATO.

(2) Access to NATO classified information applicable for the Contract (e.g. NR and above up to including NS) shall be provided only to facilities or persons whose access is necessary in connection with their involvement in the Contract. All persons who are to be given access to the information shall be informed of and acknowledge their responsibilities for protecting the information.

2.4.3 Destruction

(1) Destruction of NATO UNCLASSIFIED information is individual responsibility and shall be destroyed in a manner that it cannot be easily reconstructed in full or in part (e.g. paper copies shall be shredded before being thrown into a bin; computer disks shall be erased with NATO approved tools).

(2) The Contractor shall destroy or return any classified information provided or generated under the Contract unless the contracting authority has given written approval. Documents or other media containing NATO classified information shall be destroyed by any method approved for the destruction of classified information. The Contractor/Subcontractor shall keep a record of destruction for NATO information classified NATO CONFIDENTIAL/ NATO SECRET.

2.4.4 Unauthorised Disclosure

(1) The unauthorised disclosure of NU information shall be processed through an administrative process, and appropriate action shall be taken against those responsible. The unauthorised disclosure shall be reported to the Contractor security office.

(2) The unauthorised disclosure of information classified above NU must be reported to both the Contractor Security Office and the NCIA SO.

3. NATIONAL / NATO / INDUSTRY OFFICIALS ROLES AND RESPONSIBILITIES

3.1 National Security Authority/ Designated Security Authority

(1) The NSA/DSA is responsible for the implementation and oversight of security for NATO classified information entrusted to their contractors. The NSAs/DSAs/SAAs shall ensure that they have the means to make their security requirements upon the Contractor and that they have the right to inspect and approve the measures taken by the Contractor in compliance with Reference A for the protection of NATO classified information.

(2) The NSA/DSA of the contractor nation is responsible for ensuring that contractor's facility under its jurisdiction has adopted the protective security measures necessary to qualify for a Facility Security Clearance (FSC) and to issue security accreditation statements for the CIS that are storing, processing or transmitting classified information.

(3) In granting a FSC, the NSA/DSA shall ensure that they have the means to be advised of any circumstances that could have a bearing upon the viability of the clearance granted. This may include: a transfer or the controlling interests in the facility, a realignment of the business associations, the replacement of any of its directors, a change in its physical location, an alteration to the premises it occupies or a variation in security procedures.

3.2 Contractor and Subcontractor(s)

(1) A Facility Security Officer (FSO) shall be established for any contractor premises with an FSC. The responsibilities of the FSO shall be to coordinate all security activities to ensure compliance with NATO (and national implementation of) NATO Security policy in accordance with the provisions of the Directive on Classified Project and Industrial Security (Reference C) and are further defined in Section 3.2.1 of this document.

(2) The prime Contractor and any Subcontractor(s) are required comply with NATO security regulations as implemented by the NSA/DSA of the nation in which the work is performed, in particular, with all security requirements laid down in this Contract for handling, storing and/or transmitting NATO classified information in this PSI.

(3) The Contractor is responsible for the safeguarding of classified information, documentation, material and equipment entrusted to him or generated by him in connection with the performance of the Contract.

(4) The Contractor shall submit in due time to the NSA/DSA the personal particulars of the person the Contractor wishes to employ on the project with a view to obtaining PSCs at the required level where NC and above is involve.

(5) The Contractor shall maintain, preferably through the FSO, a continuing relationship with the NSA/DSA and / or the Contracting Authority in order to ensure that all NATO classified information involved in the bid, contract or subcontract is properly safeguarded.

(6) The Contractor, with the signature of this Contract, acknowledges receipt of these PSIs, confirms that it understands and complies with the security aspects defined within this document.

3.2.1 Facility Security Officer (FSO)

(1) An FSO shall be in place for a Contractor/Subcontractor to be granted an FSC. The FSO shall be responsible for the overall protection of NATO classified information and obliged to ensure the effective implementation of security requirements and procedures within the facility involved in any contract/subcontract requiring access to NATO classified information.

(2) The FSO shall, in accordance with national laws and regulations, serve as the main point of contact between the Contractor/Subcontractor and the Contracting Authority or relevant NSA/DSA for all security related aspects. When appointing the FSO, the following requirements apply:

e. The FSO shall be:

i. A citizen of the nation where the facility is located, or a citizen of a NATO nation;

ii. An employee of the Contractor/Subcontractor;

iii. Granted a PSC at the appropriate level;

iv. A part of the facility's management, or reporting directly to one of the members of the management in order to exercise security authority;

f. The FSO shall undertake appropriate briefing and/or training regarding protective security and threat awareness;

g. The responsible NSA/DSA should endeavour to create and maintain a close cooperation with the FSO.

(3) The FSO is responsible for the following tasks:

a. Establishing and maintaining a system of procedures and measures for the protection of NATO classified information. These measures must ensure that all security requirements specified for personnel security, physical security, security of information and CIS security (CISS) are adhered to and are in place throughout the lifetime of the classified project/contract;

b. Reporting to the responsible NSA/DSA any circumstances that may have an impact on the status of the FSC (e.g. changes in the ownership or key management personnel, changes in personnel who are involved in the classified project, changes to physical security, security of information and CISS, etc.), or PSCs (e.g. changes to or other circumstances which necessitate revalidation or which may adversely affect the individual's loyalty, reliability and trustworthiness, etc.);

c. Reporting to the responsible NSA/DSA any suspected espionage, sabotage or subversive activities at the facility, including any indication of loss, compromise or suspected compromise of NATO classified information and any other security risks concerning NATO classified information; in all cases involving compromise of NATO information, the NCIA Security Officer shall be informed.

d. Providing initial security briefings to new employees, and to all cleared persons before they are given access to NATO classified information. Providing periodic security training and security awareness programs for all personnel as required and conduct debriefings with individuals who are terminating employment on their continuing responsibilities concerning the safeguarding of NATO classified information they have accessed;

e. Conducting periodic security spot-checks or inventories as required of their facility;

f. Initiating a preliminary enquiry to ascertain the circumstances of any security violation, submit an initial investigation report of the security incident and final report including the corrective actions taken to the responsible NSA/DSA;

g. Cooperating in security inspections and investigations undertaken by the responsible NSA/DSA for assessing the protection of NATO classified information and assist in personnel security investigations of current or former employees; complying with any procedure that is, or may be, established by the NSA/DSA regarding the safeguarding and release of NATO classified information related to the contract/subcontract.

3.2.2 Facility Security Clearance

(1) The Contractor shall obtain and maintain a Facility Security Clearance (FSC) for managing, generating or having access to NATO Classified information up to and including NATO SECRET. The FSC of the Contractor's facility shall be verified through the relevant NSA/DSA. No NATO classified material are to be provided prior to this event.

3.3 Purchaser / Contracting Authority

(1) NCI Agency acts as the relevant Purchaser and Contracting Authority for this Contract.

(2) The Purchaser shall notify, via NCIA SO, the NSA/DSA of the nation with jurisdiction over the Contractor about the Contract, which involves classified information at the level NS, to include details on the nature of services or work to be performed by the Contractor, the security classification, the nature and volume of classified information to be generated and handled by the Contractor as well as any other relevant security aspects.

The Contracting Authority shall obtain the respective assurance from the responsible NSA/DSA by using the Facility Security Clearance Information Sheet (FSCIS) defined in Appendix 4 in accordance worth Reference C.

3.3.1 Personnel Security Clearances

(1) Personnel security clearances are required for access to information classified NATO CONFIDENTIAL and above. The Contractor facilities that require access to NATO CONFIDENTIAL information and above, shall be security cleared.

3.3.2 Reproduction

(1) Reproduction of documents or information classified NR may be reproduced by individuals authorised for access to the information and on equipment with controlled access.

3.3.3 Dissemination

(1) The Contractor shall limit the dissemination of NATO classified information (to include UNCLASSIFIED) to the smallest number of persons as is consistent with the proper execution of the Contract or Subcontract(s).

3.4 Security Incidents

(1) Actual or possible loss or compromise of classified information shall be reported to the relevant FSO. The FSO will report the incident to the applicable NSA/DSA and NCIA SO (Head CIS Security AMDC2), as applicable, in addition to reporting procedures prescribed by national / NATO regulations.

(2) The FSO of the facility where a violation or compromise may have occurred will investigate all such occurrences and inform their NSA/DSA of the results. NSA/DSA will promptly and fully inform other NSAs/DSAs and Air and Missile Defence Security Accreditation Board (ASAB) via the ASAB Chairman of the known details of any such occurrences, provide updates and final results on the investigation the corrective actions taken to preclude recurrences.

(3) Reports on the loss or compromise, or possible compromise, shall include as a minimum the following details:

a. A description of the circumstances.

b. The date or the period of the occurrence.

c. The date and place of discovery and location of the occurrence. The security classification and markings of the information involved in the incident.

d. Specific identification of the information or material, to include originator, subjects, reference, date, copy number, and language.

e. Assessments of the likelihood of compromise (i.e., “certain,” “probable,” “possible,” or “unlikely”).

f. A statement on whether the originator has been informed.

g. Actions taken to secure the material and limit further damage.

h. A list of the information that has been compromised or material that is unaccounted for.

i. Responsible person(s) and reasons for loss or compromise or possible loss/compromise.

(4) The above reporting requirements are in addition to any other reporting requirements of the Contracting parties, required by national regulations.

(5) Reports of investigations involving NATO CONFIDENTIAL information and above shall be provided to the NSA/DSA and the NCIA SO who will report to the NATO International Staff (IS) NATO Office of Security (NOS), if appropriate.

3.5 Termination Contract Security Procedures

(1) In the event of termination or expiration of the Contract, the Contract parties’ respective rights and responsibilities with regard to Contract information shall be determined. Retained Contract information must be safeguarded in accordance with this PSI and References A, B, I and J.

(2) Contract information and deliverables shall be protected accordingly to identified and categorised security classification levels and shall not use that information for other purposes without the prior written consent of the originating Contract parties.

(3) All NATO classified information related to the Contract shall be returned to the NCIA SO on completion or termination of their Contract unless the information has been declassified or removed from control, destroyed, or authorised for retention by the NCIA SO.

(4) In the event that a NFSC is terminated, the Contractor shall return all classified information to the NCIA SO or dispose of such information in accordance with instructions from the NCIA SO.

3.6 Security Education

(1) Contractor employees who will have access to classified and unclassified Information for the purpose of this Contract shall be briefed on or otherwise informed of, and acknowledge their understanding of their responsibilities for protecting the information. This may be accomplished by briefings, the use of written material, or by electronic means.

(2) The briefings and acknowledgements including initial, recurring, and termination actions shall be recorded in the personnel security file. The responsibilities to be presented in the briefings shall include:

a. The pertinent aspects of applicable laws and regulations;

b. The perceived threat;

c. Procedures for handling the information during use, transmission, visits, travel, and meetings;

d. How to handle possible losses or compromises and security violations ;

e. Any special security requirements that are unique to the Contract; and,

f. Penalties that may be imposed for violating the security requirements of the Contract and this PSI.

4. RELEASE OF INFORMATION

(1) The release of Contract information (classified or non-classified) to authorities or persons outside of the Contract (non-participants) without prior approval is strictly prohibited.

(2) Reference C addresses the specific procedures and arrangements for authorising the release of NATO classified information and the release authority conditions.

(3) Unless specifically authorised by the Purchaser, the Contractor shall not release any NATO information pertaining to this Contract to any third parties to whom a request to supply goods or services has been submitted.

4.1 Unilateral Release

(1) The unilateral release of classified Contract information or material to other than the Contract parties is prohibited without the specific written approval of the NCIA SO. Release of Contract classified information is restricted to the Contract parties and their (sub) contractors expressly identified and approved in writing by the NCIA SO. Contractor must ensure that subcontractors follow the same procedures.

(2) Requests for release shall be submitted to the NCIA SO in order to obtain approval from the responsible authority. Release of classified information shall be restricted to those individuals who have a need-to-know for purposes of performance on the Contract.

(3) Public release of Contract information shall receive the NCIA SO approval since it is NATO property that must be protected from unauthorised disclosure. Approval for release may also include limits, restrictions, and imposition of reasonable measures that should be taken to protect the secrecy of inventions. Although not subject to the same restrictions, handling, and transmission constraints imposed on NATO classified information, NATO unclassified information is also the property of NATO. As such, release of official information is restricted to NATO member nations only, unless written permission is received from the NCIA SO. Detailed requests for permission to release Contract information, shall be submitted to the NCIA SO before the proposed date of release.

4.2 Release of Information and Material to Third Parties

(1) No Contract information, except that which has been approved for public release may be released without the prior written approval of the NCIA SO.

4.3 Release of Contract Information at Symposia, Seminars and Conferences

(1) In accordance with Contract Part 3 Clause 12 the following shall apply:

a. Speeches and presentations by Contract parties at symposia, seminars, etc., regarding Contract must be approved in advance by the NSA/DSA, and the NCIA SO;

b. The Contractor shall submit the particulars of the meeting in advance, with sufficient time to allow NSA/DSA and the NCIA SO to ascertain the extent of the classified information access and disclosures, and determine the organisation and composition of the proposed audience;

c. Detailed requests for permission to release Contract information shall be submitted to the NCIA SO, a minimum of 45 days before the proposed date of release. Requests shall include the name of the requesting individual, date of presentation, nationality of representatives and the countries represented title of the symposium or seminar, and other information which may be required by national regulations.

4.4 Public Release of Classified Contract Information

(1) Written approval for public release of classified Contract information, including papers, advertising, brochures, displays, web pages, and other publicity material, shall be sought in writing through the NCIA SO.

(2) Contractor shall ensure that its Subcontractors follow the same procedures. The NCIA SO may reject such proposals without further recourse. Release authorisation will be made following consultation with the NSA/DSA or delegated responsible authorities.

(3) All proposals that the NCIA SO endorses will be submitted to the appropriate NSA/DSA or other NSA/DSA specified authorities. The NSA/DSA will then grant or deny release in accordance with national regulations. A minimum of 45 days should be allowed for review of the proposal.

(4) It is incumbent upon government organisations to screen all information submitted to them for public release to ensure that: (1) it is NATO UNCLASSIFIED, (2) it is technically accurate, and (3) release will not be detrimental to NATO or national security.

4.5 Exhibition Authorisation

(1) The Contractor when displaying Contract information and material at exhibitions shall have available at each exhibition a copy of the document that provides authorisation for the display. The Contractor shall ensure that all information on public display (e.g., at Air Shows, International Exhibitions, etc.) is displayed in the form in which it was officially authorised for release.

(2) The Contractor shall seek the prior written approval of the Purchaser before publishing any press release or disclosing any other information, orally or in writing, in relation to the Contract. The approval of the Purchaser shall be required for both the opportunity and the content of the information. This provision shall remain in effect after the termination of the Contract and shall cease to apply to any particular piece of information once that information becomes public knowledge other than through an act, default or omission of the Contractor or its Subcontractors.

(3) No Contract information, except that which has been approved for public release may be released without the prior written approval of the NCIA SO to third parties.

5. CHANGE PROCEDURES

(1) No changes to this document shall be made by the Contractor.

(2) The Contractor may submit, by a written order to the Purchaser, proposals for applicable changes to the relevant security instructions included in this document or changes to the Project Security Classification Guide (PSCG).

6. INTERNATIONAL HAND CARRIAGE OF NATO CLASSIFIED DOCUMENTS

6.1 Security Arrangements and Procedures

(1) Transmission of NATO UNCLASSIFIED information may be conducted through a normal mail channels or by hand carrying without formal courier orders. The information display and processing should be avoided in public places (i.e. airport, train station) and protection against potential overlooking should be satisfied.

(2) Documents or other media containing NATO classified information up to NATO RESTRICTED may be transmitted by a national mail system via registered mail, authorised messenger service or courier. Double envelopes or wrappings shall be used. The envelope or wrapping shall be opaque and shall not reveal that the package contains NATO classified information.

(3) The international transmission of material classified NATO CONFIDENTIAL and NATO SECRET shall be satisfied by an approved courier service or personal carriage by an appropriately cleared and authorised person. Receipts are required for the international transmission of NATO classified information.

(4) To meet an urgent need to transfer classified Contract documents and material between the Purchaser and Contractor and his subcontractors, the responsible NSA/DSA may approve special arrangements for hand carriage, or delivery by a national mail system or by cleared commercial delivery services.

(5) Hand carriage may be used on a case-by-case basis when government channels are not reasonably available, or transmission through government channels would result in an unacceptable delay that will adversely affect performance on the Contract, and it is verified that the information is not available at the intended destination.

(6) Classified information and material being hand carried must be sealed while in transit, may not be opened a route, and requires direct delivery from the secure facility originating point to the secure facility at the destination. During travel NATO classified information must remain in the personal custody of the carrier and be secured. It may not be left unattended in hotel rooms or vehicles and NATO classified information may not be read in public.

(7) When hand carriage of NATO classified material is permitted, the following minimum procedure shall apply:

a. The courier shall carry a Courier Certificate based on (Appendix 6), authorising him to carry the package as identified. The Courier Certificate shall be stamped and signed by the consignor’s NSA/DSA and by the consignor's FSO;

b. A copy of the "Instructions for the Courier" (Appendix 5) shall be attached to the certificate;

c. The Courier Certificate shall be returned to the issuing NSA/DSA through the consignor's Facility Security Officer (FSO) immediately after completion of the journey(s) or be kept available at the company for monitoring purposes if permitted by the issuing NSA/DSA national laws and regulations. Any circumstances that occurred during the trip which raise security concerns shall be reported by the courier on the certificate.

(8) The consignor's FSO is responsible for instructing the courier in all of his/her duties and of the provisions of the "Instructions for the Courier" (Appendix 5) and a Security Acknowledgement (Appendix 8) has to be signed.

(9) If customs authorities (of the NATO nation or of a non-NATO nation with a Security Agreement with NATO) request to examine the consignment and inspection is unavoidable, the procedures detailed in Reference C shall be followed. Customs authorities will be permitted to observe sufficient parts of the consignment to determine that it does not contain material other than that which is declared.

6.2 Handling of Classified Material as Freight

(1) The transmission of classified material as freight within a country shall be in accordance with approved national procedures providing a degree of protection not less stringent than NATO Security Policy.

7. INTERNATIONAL VISIT CONTROL PROCEDURES

7.1 Visit Types

(1) There are three types of international visits that will be used in the Contract:

a. A One-time visit is a single visit for a specific purpose and to a specific site or sites, which is not anticipated to be repeated within the same calendar year. The duration of the visit will never be longer than the validity of the personnel security clearance of the visitor(s);

b. Recurring visit is for intermittent visits over a specified period of time to a specific site or sites and for a specific purpose;

c. Emergency visit is for a one-time visit that must take place as a matter of urgency and importance and as such that the normally required lead time identified cannot be met.

d. Amendment is an extended, long-term visit for a specified period of time, subject to annual review and validation.

7.2 Recurring Visit

(1) Recurring visit covers normally the duration of a contract that requires participating personnel to make intermittent (recurring) visits to Purchaser premises.

(2) Visits covering a period of more than one year may be subject to annual review. The duration of the visit will never be longer than the validity of the personnel security clearance of the visitor(s).

(3) When Contractor personnel are required to work at the Purchaser premises during a defined time period, Purchaser authorisation is required in advance of the activity. Contractor shall coordinate arrival of its personnel with the designated and authorised NCI Agency Contract Manager (Appendix 1).

(4) The Contractor shall perform the appropriate in-processing process defined by the Purchaser Human Resources policy.

(5) The NCIA SO shall initiate an annual review to update the lists of personnel that are authorised to make recurring visits. Information concerning individuals derived from one time or emergency requests shall be added, if they are to be authorised to make recurring visits. Employees that are no longer involved in the Contract shall be deleted.

7.3 Emergency Visits

(1) An emergency visit is for a one-time visit that must take place as a matter of urgency and importance and as such that the normally required lead time identified cannot be met.

(2) Such unplanned or emergency visits should be arranged only in exceptional circumstances. To qualify as an emergency visit the following conditions must be met:

A. The visit must relate to the Contract and failure to make the visit could reasonably be expected to seriously jeopardise performance on the Contract.

B. Emergency visit requests shall be critically reviewed, fully justified and documented by the Security Officer of the requesting organisation.

C. Emergency visit requests should be submitted no less than three working days prior to the visit. Emergency visits shall be approved only as a single, one-time visit.

D. If subsequent visits are deemed necessary, the requester should submit a follow-up request for a recurring visit authorisation.

E. The requester shall co-ordinate the emergency visit in advance with the person to be visited. The requestor shall ensure that contact information is provided for both the person to be visited and a knowledgeable government point-of-contact. This contact data includes the complete name, grade or position, address, and telephone number of the person to be visited and a knowledgeable government point of contact. Provide this information in

the visit request, along with the identification of the Contract and the justification for submission of the emergency visit request.

F. Under extraordinary circumstances, an emergency visit request may be submitted with less than the required lead-time; however emergency Request for Visit (RfV) will not be accepted less than two working days prior to the start of the proposed visit.

7.4 Amendment

(1) When an already approved or pending RFV needs to be changed regarding dates, visitors and/or locations, an amendment referring to the original RFV must be submitted.

(2) Amendments to approved or pending one-time and recurring visits are authorised, provided that the amendments are limited to:

a. Change of dates of visit;

b. Addition and/or deletion of visitors; and

c. Change of location.

(3) For amendments, the standard RFV Form should be used. The type of visit cannot be changed via the amendment procedure. Amendments should refer to the original request that is still pending or already approved.

7.5 Request for Visit

(1) Visit the Purchaser facility by Contractor personnel required advance authorisation. The completed Request for Visit (RfV) format (Appendix 3) and instructions shall be used to request visit authorisation. Reference to the Contract shall be included in all visit requests. All RfVs shall be submitted through NCI Agency sponsor.

(2) For all types of visit, the standard RfV Form (see Appendix 3) should be used.

(3) This RFV Form has been designed for automated as well as manual use. However, the use of an electronic form and the transmission via e-mail are strongly encouraged.

(4) The completed RFV should be considered as an unclassified document.

8. SUBCONTRACTING

(1) Subcontracts shall not be let without the prior approval of the Contracting Authority.

(2) Subcontractor(s) are contractually obliged to comply with all the provisions of this document and any other additional security requirements issued by Contracting Authority. The Contractor shall ensure that subcontractors follow and comply with the same security procedures.

(3) Subcontractors under the jurisdiction of a NATO Nation requiring by their national laws and regulations notification of contracts involving NR shall notify their NSA/DSA about any such contracts they have been awarded.

(4) The Subcontractor(s') responsibilities include but are not limited to:

a. Obtaining NFSCs from the cognisant NSA/DSA.

b. Dissemination of information solely on the basis of the need-to-know. No person is entitled to have access to NATO classified information based on rank, status, or clearance. The individual must have a clearly demonstrated need-to-know.

9. INTERNATIONAL TRANSPORTATION

9.1 Transportation of NATO Classified Material NC or NS as Freight

(1) The consignor and the consignee of a consignment of NATO classified material to be transported as freight internationally shall jointly organise the transport arrangements. The consignor shall submit a written transportation plan to its NSA/DSA who, after consultation with the NSA/DSA of the consignee, will advise the consignor whether the transportation plan is acceptable and/or of any changes that are required.

(2) The transportation of classified material as freight within a country shall be in accordance with approved national procedures providing a degree of protection not less stringent than current NATO Security Policy.

(3) Commercial carriers can be used for transportation if it is in the opinion of the NSA/DSA concerned, in this case the following procedure shall be applied:

a. The commercial carrier shall hold an FSC if required by national laws and regulations or if it is to store NC or above at its premises;

b. The commercial carrier shall deploy personnel that have been granted a PSC at a minimum level to the material being transported;

c. Prior to any international transmission by commercial carrier, the NSAs/DSAs of the consignor and of the consignee must agree on an International Transportation Plan as described in Appendix 9 or in Reference C; and

d. When an International Transportation Plan is developed that will involve more than one international shipment of classified material, a Notice of Classified Consignment (Appendix 10 or from Reference C) shall be used to identify each shipment and provide details to the recipient, transportation personnel and any other personnel who will be involved in ensuring the security of the shipment.

9.2 Transportation of NATO Classified Material NC or NS as Freight by Road

(1) The following minimum criteria shall be applied when consignments of NATO classified material NC or NS are transported by road:

a. When storage of classified consignments is required at the carrier’s facility, the carrier shall hold an FSC at the appropriate level issued by the respective NSA/DSA;

b. Classified material shall be secured in vehicles or containers by a lock or padlock of a type currently approved by the NSA/DSA concerned. Closed vans and cars that may be sealed should be used since they offer maximum security. If this is not physically possible, the consignment should be encased to protect the classified aspects and prevent unauthorised persons from gaining access;

c. The transport shall be accompanied by at least two individuals who could be the driver, co-driver or additionally deployed security escorts or guards, and who both shall hold a PSC at the level commensurate with the classification level of the material. At least one individual shall carry a “Courier Certificate” based on (Appendix 6) and assume responsibilities of a “Courier” as described above.

d. In cases where stops must be made, arrangements shall be made in advance to use storage provided by government establishments or facilities having an appropriate FSC and the necessary cleared personnel and capabilities to ensure security of consignment. In the event such arrangements cannot be made or an emergency situation arises due to accident or breakdown of the vehicle, at least one of the security cleared individuals accompanying the material shall be responsible for keeping the consignment under constant control, and

e. Communication checks along the road shall be pre-arranged to ensure security of the consignment.

9.3 Transportation of NATO Classified Material NC or NS as Freight by Rail

(1) The following minimum criteria shall apply when consignments of NC and NS material are transported by rail:

a. Passenger accommodation shall be made available for appropriately cleared security guards or escorts who shall carry a Courier Certificate (Appendix 6 or Reference C) and assume responsibilities of a “Courier” as described above.; and

b. During stops, the security guards/escorts shall remain with the consignment.

(2) Depending on the volume of the consignment, priority shall be given to rail cars or containers that can be closed and sealed, giving maximum security.

9.4 Transportation of NATO Classified Material NC or NS as Freight by Sea

(1) The following minimum standards shall be applied when consignments of NATO material classified NC or NS are sent by sea:

a. Where possible consignments should be carried in ships sailing under the flag of a NATO nation. Ships sailing under the flag of a non-NATO nation, which represents a special security risk (as defined in the Directive on the Security of Information, "International Transmission") shall not be used. Where practicable, a guard or escort holding an appropriate PSC shall accompany the consignment;

b. Material shall be secured in locked containers approved by the NSA/DSA of the consignor. However, when this is not possible, blocked-off stowage may be approved by the NSA/DSA of the consignor. Use of security tapes or seals on the openings shall be considered. Blocked-off stowage is stowage in the hold of a ship where the material is covered and surrounded by other cargo consigned to the same destination in such a way that access to the material is physically impracticable. Where it is not possible or impracticable to carry a consignment in the hold, it may be carried as deck cargo, provided it is secured in a locked container and packaged so it is not evident that it contains classified material;

c. Stops at or entering the territorial waters of countries presenting special security risks shall normally be avoided but if unavoidable the security risk shall be assessed by the NSAs/DSAs concerned in the light of the political environment, when they receive the transportation plan drawn up by the consignor and the consignee. Unless the ship is in an emergency situation, it shall not enter the territorial waters of any of these countries;

d. Stops at any other country shall not be permitted unless the prior approval of the consignor's NSA/DSA has been obtained;

e. In all cases, loading and unloading shall be under security control; and

f. Deliveries to the port of embarkation and collection from the port of disembarkation must be so timed to prevent, as far as possible, a consignment being held in port warehouses unless the warehouse has been granted an FSC by the consignor’s or consignees NSA/DSA, as applicable. Where this is not possible, sufficient security guards must be provided to keep the consignment under adequate and permanent supervision until collection is achieved.

9.5 Transportation of NATO Classified Material NC or NS as Freight by Aircraft

(1) Preference shall be given to the use of military aircraft of a NATO nation to transport NC or NS material. If utilisation of a military aircraft of a NATO nation is not feasible, an NSA/DSA approved commercial air carrier may be used, provided it is registered in or chartered by a NATO nation. Exceptionally, airlines from non-NATO nations may also be used provided the security of the consignment can be assured by the appropriate measures taken by NSA/DSA. Scandinavian Airlines System aircraft also may be used. The following minimum standards shall be observed:

a. Every effort shall be made to deliver the consignment straight to the aircraft rather than permitting it to be stored in warehouses, etc., at airports and airfields. When a consignment cannot be loaded straight away, it shall either be stored in a NSA/DSA cleared storage

facility, or kept under guard. A sufficient number of security guards must be provided to keep the consignment under adequate and continuous supervision;

b. Every effort shall be made for the aircraft to be met on landing and the consignment to be removed at its final destination. When this is not feasible, the consignment shall be kept at the airport and a sufficient number of security guards must be provided to keep the consignment under adequate and continuous supervision;

c. Direct flights shall be used wherever possible;

d. Intermediate routine stops of short duration may be permitted, provided the consignment shall remain in the aircraft. However, if the cargo compartment is to be opened, every effort shall be made to ensure that the courier or other personnel holding an appropriate PSC are available to ensure the protection of the classified material;

e. In the event the aircraft is delayed at an intermediate stop or has to make an emergency landing, the security guard, or the person fulfilling the duties of the security guard, shall take all measures considered necessary for the protection of the consignment and if necessary seeking the assistance of his Diplomatic mission in the country concerned;

f. Transportation over countries presenting special security risks, as defined in the “Directive on the Security of Information, International Transmission” should be avoided; and

g. Stops in a non-NATO nation having a valid security agreement with NATO, may be allowed by the NSA/DSA of the consignor. Stops at airfields in non-NATO nations not having a Security Agreement with NATO, except in an emergency, shall not be permitted;

(2) When the conditions outlined below are met and if permitted by national laws and regulations, the requirements for a commercial air carrier to hold an FSC do not apply:

a. The commercial air carrier agrees to be responsible for the consignment while it is in the hold of the air plane, and will be cognisant of, and agrees to comply with the security requirements, particularly the emergency procedures specified by the NSA/DSA;

b. Consignments shall be transmitted point-to-point, the service provided by the commercial air carrier cannot be subcontracted, and the intermediate stops are not permitted;

c. A written transportation plan approved by the participating NSA/DSA shall be in place before the consignment is released to the cargo handling service or to the commercial air carrier;

d. Sufficient physical protection shall be provided to the consignment as agreed by the NSA/DSA.

(3) Companies that provide cargo handling services (such as freight forwarders) for NC and NS consignments shall have an FSC and approved protection capability if the consignment is to be stored at the facility.

10. COMMUNICATION AND INFORMATION SYSTEMS (CIS)

10.1 CIS Security Accreditation Strategy

(1) The Contractor shall use only appropriately security accredited CIS (including standalone work stations), which are used for the storing, processing or transmitting (called hereafter “handling") of NATO classified information up to and including NATO RESTRICTED and up to including NATO SECRET. The Security Accreditation shall be provided by the respective national Security Accreditation Authorities or their delegated SAAs. No CIS may be used for processing classified information without prior accreditation by the responsible authorities.

(2) The Contractor shall notify their NSA/DSA for the intended use of CIS for handling of classified information from this Contract. The Purchaser will be notified by the NSA/DSA through the FSCS in such case which will required to be accompanied from the respective accreditation statement per Contractor’s CIS.

10.2 Handling of NATO RESTRICTED and Higher Classification Information on Information and Communication Systems (CIS)

10.2.1 Requirement on Security Accreditation

(1) Security accreditation shall be performed for all contractors’ CIS that are used to handle (store, process or transmit) NATO RESTRICTED (NR) and higher classification information.

(2) This contract security clause contains the rules and regulations that shall be applied by the Contractor’s FSO or other appropriate officer to address and satisfy the minimum security requirements for the protection of NR information received or produced by the Contractor as a result of the Contract. This clause includes specific provisions to be satisfied by the Contractor under delegation from the Contracting Authority for the accreditation of the Contractor’s CIS handling NR information. Under this delegated authority the Contractor shall provide the Contracting Authority with a written statement of compliance confirming that its CIS has been accredited in compliance with the minimum requirements specified below. This written statement may be included in the Contractor’s response in acknowledgement of the receipt and requirements of this PSI.

(3) It is the responsibility of the Contractor to implement these minimum security requirements when handling classified information on its CIS.

(4) The Contractor FSO shall assess and verify the compliance of the CIS over its entire life-cycle, in order to ensure that it continues to be consistent with the requirements of this document.

(5) The following describes the minimum security requirements for handling NR information on contractors’ CIS that shall be met:

a. Protection of Hardware and Media

All mandatory Protection of Hardware and Media measures (where relevant) shall be implemented in accordance with the requirements of the Technical and Implementation Directive on CIS Security (Reference L); security measures from PHM 1-1 to PHM 8-1 inclusive.

b. Protection of Software

All mandatory Protection of Software measures (where relevant) shall be implemented in accordance with the requirements of the Technical and Implementation Directive on CIS Security (Reference L); security measures from PSW 1-1 to PSW 5-4 inclusive.

c. Protection of Services

All mandatory Protection of Services measures (where relevant) shall be implemented in accordance with the requirements of the Technical and Implementation Directive on CIS Security (Reference L); security measures from POS 1-1 to POS 7-5 inclusive.

d. Secure Maintenance

All mandatory Secure Maintenance measures (where relevant) shall be implemented in accordance with the requirements of the Technical and Implementation Directive on CIS Security (Reference L); security measures from SMT 1-1 to SMT 4-1 inclusive.

e. Network Security

All mandatory Network Security measures (where relevant) shall be implemented in accordance with the requirements of the Technical and Implementation Directive on CIS Security (Reference L); security measures from NWS 1-1 to NWS 11-7 inclusive.

f. Control Systems

All mandatory Control Systems measures (where relevant) shall be implemented in accordance with the requirements of the Technical and Implementation Directive on CIS Security (Reference L); security measures from CS 1-1 to CS 6-4 inclusive.

g. Personnel Security

All mandatory Personnel Security measures (where relevant) shall be implemented in accordance with the requirements of the Technical and Implementation Directive on CIS Security (Reference L); security measures from PS 1-1 to PS 3-2 inclusive.

h. Physical and Environmental Security

All mandatory Physical and Environmental Security measures (where relevant) shall be implemented in accordance with the requirements of the Technical and Implementation Directive on CIS Security (Reference L); security measures from PE 1-1 to PS 2-4 inclusive.

i. Data Protection

All mandatory Data Protection measures (where relevant) shall be implemented in accordance with the requirements of the Technical and Implementation Directive on CIS Security (Reference L); security measures from DA 1-1 to DA 5-2 inclusive.

j. Identity and Access Management

All mandatory Identity and Access Management measures (where relevant) shall be implemented in accordance with the requirements of the Technical and Implementation Directive on CIS Security (Reference L); security measures from IAM 1-1 to IAM 12-4 inclusive.

k. Configuration Management

All mandatory Configuration Management measures (where relevant) shall be implemented in accordance with the requirements of the Technical and Implementation Directive on CIS Security (Reference L); security measures from CM 1-1 to CM 5-3 inclusive.

l. Logging, Continuous Monitoring and Audit

All mandatory Logging, Continuous Monitoring and Audit measures (where relevant) shall be implemented in accordance with the requirements of the Technical and Implementation Directive on CIS Security (Reference L); security measures from LMA 1-1 to LMA 9-5 inclusive.

m. Incident Response

All mandatory Incident Response measures (where relevant) shall be implemented in accordance with the requirements of the Technical and Implementation Directive on CIS Security (Reference L); security measures from IR 1-1 to IR 5-4 inclusive.

n. Continuity Planning

All mandatory Continuity Planning measures (where relevant) shall be implemented in accordance with the requirements of the Technical and Implementation Directive on CIS Security (Reference L); security measures from CP 1-1 to CP 3-3 inclusive.

o. Planning Design and Implementation

All mandatory Planning Design and Implementation measures (where relevant) shall be implemented in accordance with the requirements of the Technical and Implementation Directive on CIS Security (Reference L); security measures from PDI 1-1 to PDI 5-1 inclusive.

p. Security Education and Awareness

All mandatory Security Education and Awareness measures (where relevant) shall be implemented in accordance with the requirements of the Technical and Implementation Directive on CIS Security (Reference L); security measures from EA 1-1 to EA 3-1 inclusive.

q. Interconnections to a CIS not accredited to handle NR information

(1) Security requirements, specific to interconnection scenarios, are listed in Reference J and Reference K. These Directives may be obtained from the Contracting Authority.

(2) Interconnection to another CIS, especially the internet (applicable only to NR and below), will significantly increase the threat to a Contractor's CIS and therefore the risk to the security of the NR information handled by the Contractor's CIS. A security risk assessment shall be performed to identify the additional security requirements that need to be implemented as part of the security accreditation process.

10.2.2 Disposal of IT Storage Media

(1) For IT storage media that has at any time held NR information the following sanitisation shall be performed to the entire storage media prior to disposal:

a. EEPROM and Flash Memory (e.g. USB sticks, SD cards, solid state drives, hybrid hard drives): overwrite with random data at least three times, then verify storage content matches the random data;

b. Magnetic Media (e.g. hard disks): overwrite or degauss;

c. Optical Media (e.g., CDs and DVDs): shred or disintegrate into pieces of 10mm2 or less;

d. Other storage media: seek security requirements from the Security Accreditation Authority.

(2) For IT storage media that has at any time held information classified higher than NR, seek advice from the NCIA SO for the current disposal procedures.

10.2.3 Portable Computing Devices (laptops, tablets, etc)

(1) Portable computing devices not using approved encryption shall only be used or stored in an appropriately secure location. Portable computing devices and drives containing NR or higher classification information that do not use approved encryption shall not be taken outside the Contractor's premises unless held under personal custody. The term "drives" includes all removable media. Any authentication token and/or password(s) associated with the encryption

product shall be kept separate from portable computing devices whenever it is not in use, left unattended or in transit.

10.2.4 Physical Security of CIS Handling NR information

(1) Areas in which CIS are installed to display, store, process, or transmit NR information shall be established, as a minimum, as Administrative Zones. For mobile solutions (e.g. laptop) used outside of Administrative Zones, the user shall ensure that the displayed content is protected in a way that NR information is not exposed to unauthorised individuals.

(2) CIS areas housing servers, network management system, network controllers and communications controllers should be established as separate and controlled areas with an appropriate access control system. Access to these CIS areas should be limited to only specifically authorised persons.

10.2.5 Security of NR Removable Computer Storage Media

(1) Removable computer storage media containing NR information are required to be labelled with that classification marking. Measures shall be in place to prevent unauthorised access to NR removable computer storage media in order to maintain the need-to-know principle

10.2.6 Use of CIS Equipment Privately Owned by Contractor's Personnel

(1) The use of privately-owned equipment of Contractor's personnel (hardware and software) for processing NR information shall not be permitted

10.2.7 CIS Users' responsibilities

(1) CIS users (e.g. end users, administrators) involved in the handling of NR information within the CIS shall be made aware of their responsibilities and the procedures to be followed. The responsibilities and the procedures to be followed shall be documented and acknowledged by CIS users in writing.

10.2.8 Advice

(1) Advice or clarification of the provisions of this contract security clause shall be obtained from the Contracting Authority.

10.2.9 Audit/inspection

At the request of the contracting authority or relevant NSA/DSA/SAA, the Contractor shall provide evidence of compliance with this Contract Security Clause and permit an audit of inspection of the Contractors processes and facilities by representatives of the contracting authority or the contractors NSA/DSA or relevant NATO security authorities to ensure compliance with these requirements.

10.3 Handling Of NATO CONFIDENTIAL/SECRET Information on Information and Communication Systems (CIS)

(1) All Contractor's CIS storing and processing NATO CONFIDENTIAL and higher information shall be subject to a formal security accreditation process in accordance with Section 10.1.1.

(2) The requirements listed in Section 10.2.1 are applicable to all NS CIS. Additional requirements shall be adhered to as specified by the respective NSA/DSA and in accordance with the security requirements found in the Reference L.

10.4 Electronic Transmission of NATO Information

(1) Electronic transmission of NATO UNCLASSIFIED information may be conducted over Internet on the condition that only recognised business e-mail addresses are used for a distribution (e.g. sender and addressee - e.g. @ncia.nato.int).

(2) Storing NATO UNCLASSIFIED or higher information on portals accessible through the internet is strictly forbidden.

(3) Electronic transmission of NATO RESTRICTED information may be performed over accredited CIS or interconnecting CIS, which for this Contract is the NR AIS and the AIDES. Transmission of classified information NATO CONFIDENTIAL and above is strictly forbidden over NR AIS system.

(4) Electronic transmission of NATO CONFIDENTIAL information may be performed over accredited CIS or interconnecting CIS, which for this Contract is the AIDES.

(5) Requests for NR AIS laptops, accounts and iron-keys should be directed in writing to the NCIA Project Manager or through a NCI Agency Customer Request Form (CRF). Before NR AIS account creation, the involved user shall read the related NR AIS Security Operating Procedures (SecOPs) and acknowledge in writing the required adherence and compliance (Reference M).

(6) Standard telephone or facsimile system shall be used to exchange only NATO UNCLASSIFIED information.

11. SECURITY CLASSIFICATION GUIDE

(1) The Security Classification Guide (SCG) (Reference S), and changes thereto, are the basis for classification, re-grading, or declassification of Contract Information and/or material. It constitutes the authority that shall be cited as the basis for initial classification, re-grading, or declassification of Contract Information or material concerning the Contract. Security classification must be determined by considering all applicable information and references.

(2) If the appropriate classification is unclear, the matter shall be referred to the NCIA SO. Questions concerning the content and interpretation as well as proposed changes to the classification guide will be co-ordinated by the NCIA SO. Until the matter is resolved, the classification level assigned should be the highest anticipated.

Appendix 1. CONTACT INFORMATION

(1) Contracting Authority (Purchaser)

Name	Mr Martin Steenwege
Function	Senior Contracting Officer
Telephone	+32 2 707 8335
Address	NATO HQ Boulevard Leopold III, B-1110 Brussels, Belgium
E-mail	martin.steenwege@ncia.nato.int

(2) NCIA Security Officer

Name	Eur Ing Dr Kevin MEPHAM
Function	CIS Security Section (NCIA AMDC2)
Telephone	+31 70 374 1760
Address	NCI Agency, Oude Waalsdorperweg 61, 2597 AK, The Hague, Netherlands
E-mail	Kevin.mepham@ncia.nato.int

(3) Purchaser (NCI Agency) Project Manager

Name	Alberto Bellini
Function	Project Manager
Telephone	+31 70 374 3268
Address	NCI Agency, Oude Waalsdorperweg 61, 2597 AK, The Hague, Netherlands
E-mail	Alberto.Bellini@ncia.nato.int

(4) Contractor Contract Manager

Name	TBD
Function	
Telephone	
Address	
E-mail	

(5) Contractor Security Officer

Name	TBD
Function	
Telephone	
Address	
E-mail	

(6) Contractor CIS Officer

Name	TBD
Function	
Telephone	
Address	
E-mail	

(7) National Security Agency

Name	TBD
Telephone	
Address	
E-mail	

(8) Delegated Security Agency

Name	TBD
Telephone	
Address	
Name	
Telephone	
Address	

Appendix 2. MARKING NATO INFORMATION

(1) Each document (electronic or physical) shall be conspicuously marked or stamped at the top and bottom of the front cover and all pages and the back side of the last page and back side of the back cover with the security classification (e.g., “NATO RESTRICTED”).

(2) "Classified by", Downgrade to”, or “Declassify on” markings together with the agreed dates for the action, shall be annotated on the front lower left cover of documents.

(3) The overall classification of each page shall be reflected at the top and bottom of each page. The classification marking shall reflect the highest level of classified information on that page. The level of classification of information in the paragraphs or portion of information on each page shall be adequately identified in accordance with the paragraph and portion-marking requirement outlined below.

(4) Paragraph or portion markings of information in NATO classified documents shall be as follows:

a. (NU) for NATO UNCLASSIFIED

b. (NR) for NATO RESTRICTED

c. (NC) for NATO CONFIDENTIAL

d. (NS) for NATO SECRET

Appendix 3. INSTRUCTIONS FOR USE AND COMPLETION OF A REQUEST FOR VISIT

1. General Instruction

(1) The Request for Visit (RFV) must be completed without misstatement or omission. Failure to provide all requested information will delay the processing and possibly lead to the denial of the request.

(2) This RFV should be typed. Electronic processing and transmitting of the RFV is encouraged. The completed RFV is normally an unclassified document. The completion of the RFV Form should be in either one of the official NATO languages.

(3) RFV must be in the possession of the receiving host NSA/DSA in accordance with the RFV lead times detailed in Paragraph 3.

(4) The completed RFV has to be submitted to the Security Officer of the requesting agency, organisation or facility. After completion by the Security Officer of the requesting agency, organisation or facility, the RFV should be sent to the following national agency's address that will process the request (to be inserted by issuing NSA/DSA):

Name of Agency	
Address:	
Fax no:	
E-mail address:	

2. Detailed Instructions for Completion of Request for Visit

(1) These detailed instructions are guidance for the visitors and the Security Officers who complete the RFV.

HEADER	Insert full country or international organisation name (e.g. NATO CI Agency, NATO International Military Staff, SHAPE, etc) of the host
1.TYPE OF VISIT REQUEST	Select the appropriate checkbox for the type of visit request. If the Emergency checkbox is selected, complete the remarks portion in item 15 of the RFV Form to explain the reasons behind the emergency RFV. If the Amendment checkbox is selected, mark the appropriate checkbox for the type of amendments and insert the reference number provided by the NSA/DSA of the original RFV that the amendment is made to. Depending on the laws/regulations of the countries involved, a one-time visit request which is issued for the posting of personnel may require additional information/documents to be included with the RFV Form.
2. TYPE OF INFORMATION/ MATERIAL OR SITE ACCESS	Select the appropriate checkbox for the type of information/material or site access. The first box covers direct access to information/material classified NC or above. The second box shall be checked when unescorted access to Security Areas (e.g. Class I/II) is required but no direct access to information/material classified NC or above is anticipated.
3. SUMMARY	Insert the number of sites to be visited and the number of visitors.
4. ADMINISTRATIVE DATA	DO NOT FILL IN - LEAVE BLANK *To be completed by requesting NSA/DSA if required*
5. REQUESTING GOVERNMENT AGENCY, ORGANISATION OR INDUSTRIAL FACILITY	Select the appropriate checkbox (only one box) for the entity of the requesting government agency, organisation or industrial facility. Insert the full name, full postal address (include city, province/state, and postal zone), e-mail address, facsimile number and telephone number.

6. GOVERNMENT AGENCY(IES), ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED	Complete Annex 1 to the RFV Form to include information on all of the sites to be visited.
7. DATE OF VISIT	Insert the period of the visit by using numeral “day/month/year” (dd/mm/yyyy).
8. TYPE OF INITIATIVE	Select one item from each column as indicated
9. IS THE VISIT PERTINENT TO	Select the appropriate checkbox and specify the full name of the government project/programme. Foreign Military Sales case, etc., or request for proposal or tender offer. Abbreviations should be avoided.
10.SUBJECT TO BE DISCUSSED/ JUSTIFICATION/ PURPOSE	Give a brief description of the subject(s) motivating the visit. If known, include the details of the host Government/Project Authority and solicitation/ contract number. Abbreviations should be avoided. Remarks: In case of a recurring visit, this item of the RFV Form should state "Recurring Visits" as the first words in the data element (e.g. Recurring Visits to discuss...). It is strongly advised to repeat the subject to be discussed and/or the justification of the visit in the language of the receiving country. Make sure to describe the subject to be discussed in a way that it does not reveal any classified information since the completed RFV is considered to be an UNCLASSIFIED document.
11.ANTICIPATED HIGHEST LEVEL OF INFORMATION/ MATERIAL OR UNESCORTED ACCESS TO SECURITY AREAS	Select the appropriate checkbox for the anticipated highest level of information/material or unescorted access to security areas. If the box “Other” is checked, it shall be specified.
12.PARTICULARS OF VISITOR(S)	Complete Annex 2 to the RFV Form to include information on all of the visitors. When there is more than one visitor, enter the visitors’ surnames in alphabetic order if possible
13.THE SECURITY OFFICER OF THE REQUESTING AGENCY, ORGANISATION OR INDUSTRIAL FACILITY	This item requires the name, telephone number, e-mail address, and signature of the requesting Security Officer.
14. CERTIFICATION OF SECURITY CLEARANCE LEVEL	DO NOT FILL IN - LEAVE BLANK To be completed by government/NATO certifying authority only. In accordance with the laws/regulations of the countries involved, government certifying authority must also complete this item for RESTRICTED. Note for the certifying authority: Insert name, address, telephone number, and e-mail address. Date and signature. If the certifying authority corresponds with the requesting National Security Authority, insert in this item: “See item 14 of the RFV Form”. Remark: Items 13 and 14 of the RFV Form may be completed by the appropriate official of the Embassy of the requesting country as per national legislations, policies or directives.

15.REQUESTING SECURITY AUTHORITY	DO NOT FILL IN - LEAVE BLANK To be completed by the requesting NSA/DSA or responsible NATO security office only as per below instructions. Insert name, address, telephone number, and e-mail address. Date and signature.
16.REMARKS	In case of an emergency visit, it is mandatory to give the reasons for the emergency visit in this field of the RFV Form. The particulars of the knowledgeable person, see Paragraph 7.4, should also be identified in this field of the RFV Form. This item can be used for certain administrative requirements (e.g. proposed itinerary, request for hotel, and/or transportation, etc.). This space is also available for the receiving NSA/DSA for processing (e.g., “no security objections”, etc.). In case a special briefing is required, the type of briefing and the date that the briefing was given should be stated.

ANNEX 1 TO RFV FORM	
GOVERNMENT AGENCY(IES), ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED	Select the appropriate checkbox (only one box) for the government agency, organisation or industrial facility to be visited. Repeat for every site to be visited. Insert the full name, full physical address (include city, province/state, and postal zone), telephone number and facsimile number. Insert the name, e-mail and telephone number of the main point of contact or the person with whom the appointment for the visit was made. Insert the name, e-mail and telephone number of the Security Officer or the secondary point of contact. Remarks: For visits to the United States, one RFV Form with Annexes for each agency/organisation/facility to be visited should be filled in. For visits to military sites in the United States, it is mandatory to specify which military unit will be visited (e.g. Army, Air Force, Navy, Marine Corps or Defence Intelligence Agency).

ANNEX 2 TO RFV FORM	
PARTICULARS OF VISITOR(S)	Select the appropriate checkbox (only one box) for the type of employment of the visitor (e.g. military, defence public servant, government, industry/embedded Contractor, international organisation employee (e.g. NATO, EU, etc.). Repeat for every visitors. Surname: Family name. Forenames: As per passport. Rank: Insert the rank of the visitor if applicable. DOB: Insert date of birth by using numeral “day/month/year” (dd/mm/yyyy). POB: Place of birth (city-province/state-country). Nationality: Insert nationality as per passport. Security clearance level: Actual security clearance status (e.g. TS, S, C). Indicate NATO clearance (CTS, NS, NC) if the visit is related to NATO business. PP/ID Number: Enter the passport number or identification card number, as required by host government. Position: Insert the position the visitor holds in the organisation (e.g., director, product manager, etc.) Company/Agency: Insert the name of the government agency, organisation, or industrial facility that the visitor represents.

Visit Notification Form

All fields must be completed.

<table>
<tr><td colspan="3">REQUEST FOR VISIT

TO:_____
(Country/NATO body)</td></tr>
<tr><td>1. TYPE OF VISIT REQUEST</td><td>2. TYPE OF INFORMATION/ MATERIAL OR SITE ACCESS</td><td>3. SUMMARY</td></tr>
<tr><td>☐ One-time
☐ Recurring
☐ Emergency
☐ Amendment
☐ Dates
☐ Visitors
☐ Agency/Facility

For an amendment, insert the NSA/DSA original RFV Reference No._____</td><td>☐ NATO CONFIDENTIAL or above, or
☐ access to security areas.</td><td>No. of sites: _____
No. of visitors:_____</td></tr>
<tr><td colspan="3">4. ADMINISTRATIVE DATA:</td></tr>
<tr><td colspan="2">Requestor:

To:</td><td>NSA/DSA RFV Reference No._____

Date (dd/mm/yyyy):_____/_____/_____</td></tr>
<tr><td colspan="3">5. REQUESTING GOVERNMENT AGENCY, ORGANISATION OR INDUSTRIAL FACILITY:

☐ Military ☐ Government ☐ Industry ☐ NATO ☐ Other: _____

NAME:

POSTAL ADDRESS:
E-MAIL ADDRESS:

FAX NO: TELEPHONE NO:</td></tr>
<tr><td colspan="3">6. GOVERNMENT AGENCY(IES) , ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED - (Annex 1 to be completed)</td></tr>
<tr><td colspan="3">7. DATE OF VISIT (dd/mm/yyyy): FROM_____/_____/_____TO_____/_____/_____</td></tr>
<tr><td colspan="3">8. TYPE OF INITIATIVE (Select one from each column):</td></tr>
<tr><td colspan="2">☐ Government initiative
☐ Commercial initiative</td><td>☐ Initiated by requesting agency or facility
☐ By invitation of the facility to be visited</td></tr>
</table>

9. IS THE VISIT PERTINENT TO:

☐ Specific equipment or weapon system
☐ Foreign military sales or export licence
☐ A programme or agreement
☐ A defence acquisition process
☐ Other

Specification **of the selected subject:**

10. SUBJECT TO BE DISCUSSED/JUSTIFICATION/PURPOSE ***(To include details of host Government/Project Authority and solicitation/contract number if known and any other relevant information. Abbreviations should be avoided)*****:**

11. ANTICIPATED HIGHEST LEVEL OF INFORMATION/MATERIAL OR UNESCORTED ACCESS TO SECURITY AREAS

☐ NATO CONFIDENTIAL ☐ NATO SECRET

☐ COSMIC TOP SECRET ☐ Other

If other, specify*:*_____

12. PARTICULARS OF VISITOR(S) - ***(Annex 2 to be completed)***

13. THE SECURITY OFFICER OF THE REQUESTING GOVERNMENT AGENCY, ORGANISATION OR INDUSTRIAL FACILITY:

NAME:

TELEPHONE NO:

E-MAIL ADDRESS:

SIGNATURE:

14. CERTIFICATION OF SECURITY CLEARANCE LEVEL: NAME: ADDRESS: TELEPHONE NO: E-MAIL ADDRESS: SIGNATURE: DATE *(dd/mm/yyyy)*:_____/_____/_____
15. REQUESTING NATIONAL SECURITY AUTHORITY/DESIGNATED SECURITY AUTHORITY/*NATO security office*: NAME: ADDRESS: TELEPHONE NO: E-MAIL ADDRESS: SIGNATURE: DATE *(dd/mm/yyyy)*:_/_____/_____
16. REMARKS *(*Mandatory justification required in case of an emergency visit):

1. **ANNEX 1 to RFV FORM**

GOVERNMENT AGENCY(IES), ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED
1. ☐Military ☐Government ☐Industry ☐NATO ☐Other:_____ NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO: 2. ☐Military ☐Government ☐Industry ☐NATO ☐Other:_____ NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO:

GOVERNMENT AGENCY(IES), ORGANISATION(S) OR INDUSTRIAL FACILITY(IES) TO BE VISITED
3. ☐Military ☐Government ☐Industry ☐NATO ☐Other: _____ NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO:
4. ☐Military ☐Government ☐Industry ☐NATO ☐Other: NAME: ADDRESS: TELEPHONE NO: FAX NO: NAME OF POINT OF CONTACT: E-MAIL: TELEPHONE NO: NAME OF SECURITY OFFICER OR SECONDARY POINT OF CONTACT: E-MAIL: TELEPHONE NO: ***(Continue as required)***

2. **ANNEX 2 to RFV FORM**

PARTICULARS OF VISITOR(S)	
1. ☐Military ☐Contractor's Personnel ☐NATO ☐Other IO (Specify:_____)	☐Government
SURNAME: FORENAMES *(as per passport)*: RANK *(if applicable)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/AGENCY:	
2. ☐Military ☐Contractor's Personnel ☐NATO ☐Other IO (Specify:_____)	☐Government
SURNAME: FORENAMES *(as per passport)*: RANK *(if applicable)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/AGENCY:	

PARTICULARS OF VISITOR(S)
3. ☐Military ☐Government ☐Contractor's Personnel ☐NATO ☐Other IO (Specify:_____) SURNAME: FORENAMES *(as per passport)*: RANK *(if applicable)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/AGENCY:
4. ☐Military ☐Government ☐Contractor's Personnel ☐NATO ☐Other IO (Specify:_____) SURNAME: FORENAMES *(as per passport)*: RANK *(if applicable)*: DATE OF BIRTH *(dd/mm/yyyy)*:____/____/____ PLACE OF BIRTH: NATIONALITY: SECURITY CLEARANCE LEVEL: PP/ID NUMBER: POSITION: COMPANY/AGENCY: ***(Continue as required)***

3. International Visits Processing Times/Lead Times and NU or NR Notification Requirements

(1) The national requirements for RFV for NU or NR notification shall not put additional obligations on other NATO nations or Contractors under their jurisdiction.

a. The following table depicts the number of working days prior to the date of the one-time visit or the date of the first recurring visit that the request should be in the possession of the receiving host NSA/DSA.

b. Visits involving NR information will be arranged directly between the SO responsible for the visitor and the SO of the facility to be visited without formal requirements. The SO of the facility to be visited should be asked if a request for visit is required to be provided to its NSA/DSA and if so, the SO of the facility to be visited should submit a visit request to its NSA/DSA on behalf of the visitor. However, visitors are not required to hold a PSC.

COUNTRY	RFV REQUIRED		NUMBER OF WORKING DAYS	
	Unclassified Visits	Restricted Visits	Request	Amendment/ Change
Albania	No	Yes	20	10
Belgium	No	No	20	09
Bulgaria	No	Yes	20	No deadline
Canada	Yes 1. May be required for governmental facilities 2. Required for military facilities	Yes 1. May be required for governmental facilities 2. Required for military facilities	20	10
Croatia	No	No	20	7
Czech Republic	No	Yes	20	10
Denmark	No	No	07	05
Estonia	No	Yes	20	05
France	No	No	15	05
Germany	No	No	20	10
Greece	Yes 1. May be required for governmental facilities 2. Required for military facilities	Yes 1. May be required for governmental facilities 2. Required for military facilities	20	10
Hungary	No	No	20	10
Iceland	-	-	-	-
Italy	No	Yes	20	07
Latvia	No	No	20	05
Lithuania	No	Yes	20	10
Luxembourg	No	Yes	20	09
Netherlands	No	Yes required for military facilities only	10	05
Norway	No	Yes	10	05
Poland	No	No	25	10
Portugal	No	No	21	07

COUNTRY	RFV REQUIRED		NUMBER OF WORKING DAYS	
	Unclassified Visits	Restricted Visits	Request	Amendment/ Change
Romania	No	No	25	10
Slovakia	No	No	20	10
Slovenia	No	Yes	21	07
Spain	No	No	20	08
Turkey	Yes For military facilities only	Yes For military facilities only	21	10
United Kingdom	No	No	20	05
United States	No	Yes	21	05

4. List of Authorities concerned with IVCPs

COUNTRY	OFFICE	E-mail
Albania	NSA	E-mail: Sektretaria.nsa@mod.gov.al Tel: +335 4 224 5995
Belgium		
Bulgaria	State Commission on Information Security (NSA)	E-mail: dksi@government.bg
Canada	Industrial Security Sector, Public Works and Government Services Canada, Designated Security Authority (DSA).	E-mail: ssivisites.issvisits@pwgsc.gc.ca
Croatia	NSA/DSA, Office of the National Security Council	E-mail: ivcp@uvns.hr
Czech Republic	NSA	E-mail: posta@nbu.cz
Denmark	Danish Defence Intelligence Service (NSA for the Military Sphere)	E-mail: fe4222@fe-ddis.dk
Estonia	NSA	E-mail: nsa@mod.gov.ee
France	MOD acting as DSA	E-mail: In: Bagneux.sdi–sii@dga.defense.gouv.fr Out: bagneux.sdi-visit@dga.defense.gouv.fr
Germany	RFV's relating to military projects: Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support Division Z1.3 RFV's relating to civil projects: Federal Ministry for Economic Affairs and Energy (DSA) Division - ZB2	E-mail: baainbwZ1.3-bkv@bundeswehr.org Tel.: +49.261.400.13190/13192 Fax: +49.261.400.13189 E-mail: zb2-international@bmwi.bund.de Tel.: +49 228 99615 3621/3605 Fax: +49 228 99615 2603

COUNTRY	OFFICE	E-mail
Greece	Hellenic National Defence General Staff F' Division Security Directorate - Industrial Security Office	E-mail: daa.industrial@hndgs.mil.gr Tel: 00 30 210 6572022 Fax: 0030 210 6527612
Hungary	NSA	E-mail: nbf@nbf.hu Tel.: +36.17.95.23.03 Fax: +36.17.95.03.44
Iceland		
Italy	Dipartimento delle Informazioni per la Sicurezza – Ufficio Centrale per la Segretezza	E-mail: mg3437.a03@alfa.gov.it
Latvia	The Constitution Protection Bureau (SAB)	E-mail : ndi@sab.gov.lv
Lithuania	Commission for Secrets Protection Co-ordination	E-mail: nsa@vsd.lt Tel.: +370 706 66701(03) +370 706 66708 Fax: +370 706 66700
Luxembourg	Autorité nationale de Sécurité 207, route d'Esch L-1471 Luxembourg	E-mail: ans@me.etat.lu Tel.: +352.24.78.2210 Fax.: +352.24.78.2243
Netherlands	NSA/DSA	E-mail: NSA: NIVCO@minbzk.nl DSA: indussec@mindef.nl*
Norway	The Norwegian Defence Security Agency	E-mail: fsa.kontakt@mil.no
Poland	NSA	E-mail: nsa@abw.gov.pl
Portugal	NSA/GNS –Rua da Junqueira, 69, 1300-342 Lisboa	E-mail: geral@gns.gov.pt
Romania	National Registry Office for Classified Information (ORNISS)	E-mail: relatii.publice@orniss.ro
Slovakia	NSA	E-mail: podatelna@nbusr.sk
Slovenia	NSA	E-mail: gp.uvtp@gov.si

COUNTRY	OFFICE	E-mail
Spain	NSA	E-mail: sp-ivtco@areatec.com
Turkey		
United Kingdom	Defence Equipment and Support PSyA, Ministry of Defence, International Visits Control Office, Poplar-1 # 2004, Abbey Wood, Bristol, England, BS34 8JH, UK	Email: Desinfra-ivco@mod.uk Tel.: + 44 117 91 33840 Fax.: + 44 117 91 34924
United States	For Department of Defense: Mr. Mario Rubio International Security Directorate Office of the Under Secretary of Defense (Policy) Defense Technology Security Administration 4800 Mark Center Drive Suite 07E12 Alexandria, VA 22350	E-mail: Mario.rubio@dtsa.mil Tel.: +1.571.372.2561 Fax.: +1 571.372.2559

Appendix 4. FACILITY SECURITY CLEARANCE INFORMATION SHEET (FSCIS)[1]

REQUEST FOR A FACILITY SECURITY CLEARANCE ASSURANCE TO : _____ (NSA/DSA Country name)
Please complete the reply boxes, where applicable: [ ] Provide an FSC assurance at the level of: [ ] NATO SECRET for the facility listed below [ ] Including protecting of classified material/information [ ] Including Communication and Information Systems (CIS) for processing classified information [ ] Initiate an FSC up to and including the level of ..... with …….level of protection and ……..level of CIS, if the facility does not currently hold these levels of capabilities.
Confirm accuracy of the details of the facility listed below and provide corrections/additions as required.
1. Full facility name: …… 2. Full facility address: …… 3. Mailing address (if different from 2.) …… 4. Zip/postal code / city / country …… 5. Name of the Security Officer …… 6. Telephone/Fax/E-mail of the Security Officer …… Corrections / additions: …….. …….. …….. …….. …….. …….. …….. 7. This request is made for the following reason(s): (indicate particulars of the pre-contractual stage, contract, subcontract, programme/project): ……..…… ……..……\ Requesting NSA/DSA/NPA/NPO: Name: …… Date: (*dd/mm/yyyy*) ……
REPLY (within 5 working days)
This is to certify that the above mentioned facility: 1. [ ] holds an FSC up to and including the level of: [ ] TS [ ] CTS [ ] S [ ] NS [ ] C [ ] NC [ ] Other: …….. 2. [ ] on the above mentioned request, the FSC process has been initiated. You will be informed when the FSC has been granted or refused.

[1] All fields must be completed and the form communicated via Government-to-Government or Government to International Organisation channels.

3. [ ] does not hold an FSC.

4. has the capability to protect classified information/material:

[ ] yes, level: ……..……. [ ] no

5. has Accredited CIS:

[ ] yes, level: ……..……. [ ] no

6. This FSC assurance expires on …….. (*dd/mm/yyyy*), or as advised otherwise by the NSA/DSA.

In case of an earlier invalidation or in case of any changes of the information listed above you will be informed.

7. Remarks:

…….....….

…….....……

Issuing NSA/DSA:

Name: …….. Date: (*dd/mm/yyyy*).....……

Appendix 5. INSTRUCTIONS FOR THE COURIER

Annex to the "Courier Certificate", No. …….
for the International Hand Carriage of Classified Material

INSTRUCTIONS FOR THE COURIER

(1) You have been appointed to carry/escort a classified consignment. Your "COURIER CERTIFICATE"/"MULTI-TRAVEL COURIER CERTIFICATE" (Appendix 6 / Appendix 7) has been provided. Before starting the journey, you will be briefed on the security regulations governing the hand carriage of the classified consignments and on your security obligations during the specific journey (behaviour, itinerary, schedule, etc.). You will also be requested to sign a declaration that you have read and understood and will comply with prescribed security regulations.

(2) The following general points are brought to your attention:

a. You will be held liable and responsible for the consignment described in the Certificate;

b. Throughout the journey, the classified consignment must stay under your personal control;

c. The consignment will not be opened a route except in the circumstances described in sub-paragraph (j) below;

d. The classified consignment is not to be discussed or disclosed in any public place;

e. The classified consignment is not, under any circumstances, to be left unattended. During overnight stops, military facilities or industrial companies having appropriate security clearance may be utilised. You are to be instructed on this matter by your facility Security Officer;

f. While hand carrying a classified consignment, you are forbidden to deviate from the travel schedule provided;

g. In cases of emergency, you must take such measures as you consider necessary to protect the consignment, but on no account will you allow the consignment out of your direct personal control; to this end, your instructions include details on how to contact the security authorities of the countries you will transit as listed in sub-paragraph (l) below. If you have not received these details, ask for them from your facility Security Officer;

h. You and the facility Security Officer are responsible for ensuring that your personal expatriation and travel documentation (passport, currency and medical documents, etc.) are complete, valid and current;

i. If unforeseen circumstances make it necessary to transfer the consignment to other than he designated representatives of the company or government you are to visit, you will give it only to authorised employees of one of the points of contact listed in sub-paragraph (l);

j. There is no assurance of immunity from search by the Customs, Police, and/or Immigration Officials of the various countries whose borders you will be crossing; therefore, should such officials enquire into the contents of the consignment, show them your Certificate and this note and insist on showing them to the actual senior Customs, Police, and/or Immigration Official; this action should normally suffice to pass the consignment through unopened. However, if the senior Customs, Police, and/or Immigration Official demands to see the actual contents of the consignments you may open it in his presence, but this should be done in an area out of sight of the general public;

You should take precautions to show officials only as much of the contents as will satisfy them that the consignment does not contain any other item and ask the official to repack or assist in repacking it immediately upon completion of the examination. You should request the senior Customs, Police, and/or Immigration Official to provide evidence of the opening and inspection of the packages by signing and sealing them when closed and confirming in the shipping documents (if any) that the consignment has been opened.

If you have been required to open the consignment under such circumstances as the foregoing, you must notify the receiving facility Security Officer and the dispatching facility

Security Officer, who should be requested to inform the NSA/DSA of their respective government.

k. Upon your return, you must produce a bona fide receipt for the consignment signed by the Security Officer of the facility or agency receiving the consignment or by an NSA/DSA of the receiving government;

l. Along the route you may contact the following officials to request assistance:

……

……

……

……

……

……

Appendix 6. COURIER CERTIFICATE

[LETTERHEAD] COURIER

CERTIFICATE PROGRAMME

TITLE (optional)

COURIER CERTIFICATE NO. …….. (*)

FOR THE INTERNATIONAL HAND CARRIAGE OF CLASSIFIED DOCUMENTS, EQUIPMENT AND/OR COMPONENTS

This is to certify that the bearer: Mr./Ms. (name/title):

born on: (day/month/ year), in (country): a national of (country):

holder of passport/identity card no.: (number) issued by: (issuing authority)

on: (day/month/year)

employed with: (company or organisation)

is authorised to carry on the journey detailed below the following consignment:

(Number and particulars of the consignment in detail, i.e., No. of packages, weight and dimensions of each package and other identification data as in shipping documents)

…….

…….

* May also be used by security guards.

The attention of Customs, Police, and/or Immigration Officials is drawn to the following:

- The material comprising this assignment is classified in the interests of the security of:

(NATO, the country of origin of the shipment and that of the destination shall be indicated. The country(ies) to be transited also may be indicated).

- It is requested that the consignment will not be inspected by other than properly-authorised persons or those having special permission.

- If an inspection is deemed necessary, it is requested that it be carried out in an area out of sight of persons who do not belong to the service and, in the presence of the courier.

- It is requested that the package, if opened for inspection, be marked after re-closing, to show evidence of the opening by sealing and signing it and by annotating the shipping documents (if any) that the consignment has been opened.

- Customs, Police, and/or Immigration Officials of countries to be transited, entered or exited are requested to give assistance, if necessary, to ensure successful and secure delivery of the consignment.

Appendix 7. MULTI-TRAVELS COURIER CERTIFICATE

[LETTERHEAD]

PROGRAMME TITLE (optional)

MULTI-TRAVELS COURIER CERTIFICATE N° …….

FOR INTERNATIONAL HAND CARRIAGE OF CLASSIFIED DOCUMENTS,

EQUIPMENTS AND/OR COMPONENTS

This is to certify that the bearer

Mr/Ms (name/title)

born on (day/month/year) …… in (country) ……..……,

a national of (country) ……..

holder of passport or identity card n° ……

issued by (issuing authority): ……

on (day/month/year):……

employed with (facility): ……..……...

is authorised to carry the classified documents, equipments and/or components between the following countries:……..……..……...

The bearer above is authorised to use the present certificate as many times as necessary, for classified shipments between the countries here above until (day / month / year): ……

Each sending is attached with the shipment description.

The attention of Customs, Police and/or Immigration Officials is drawn to the following:

- The material comprising each consignment is classified in the interest of the security of:

  (NATO, the country of origin of the shipment and that of the destination shall be indicated. The country (ies) to be transited also may be indicated).

- It is requested that the consignment will not be inspected by other than properly authorised persons or those having special permission.
- If an inspection is deemed necessary, it is requested that it be carried out in an area out of sight of persons who do not belong to the service and, in the presence of the courier.

It is requested that the package, if opened for inspection, be marked after re-closing, to show evidence of the opening by sealing and signing it and by annotating the shipping documents (if any) that the consignment has been opened.

Customs, Police and/or Immigration Officials of countries to be transited, entered or exited are requested to give assistance, if necessary, to ensure successful and secure delivery of the consignment.

Instructions for the Courier (Appendix 7) are also applicable.

Attachment to multi-travels courier certificate No:.....

Description of consignment nr: ……..

Transport from (**day/month/year**): …… to (**day/month/year**):

…… Bearer (name): ……

Itinerary: from (originating country) …… to (destination country)
…… through (crossed countries) ……

authorised stops (list of locations):

…… References of receipt or

inventory list:

Description of the consignment (number of package, dimensions and, if needed, weight of each package):

Officials you may contact to request assistance

Signature of the consignor's security officer …….	Signature of the NSA/DSA …….
Facility stamp …….	Official stamp or NSA/DSA's seal …….

Note to be signed on completion of each journey:

I declare in good faith that, during the journey covered by this "shipment consignment", I am not aware of any occurrence or action, by myself or by others, that could have resulted in the compromise of the consignment.

Courier's signature: ……..

Witnessed by (name and signature of consignor's security officer):

……. Date of return of the "shipment consignment"

(day/month/year): ……

Appendix 8. SECURITY ACKNOWLEDGEMENT (IN CASE OF HAND CARRIAGE)

[LETTERHEAD]

SECURITY ACKNOWLEDGEMENT

DECLARATION

(name, forename)

(name of company)

(position in company)

I have been briefed on and provided with instructions concerning the handling and custody of classified documents/equipment to be carried by me. I have read and understood their contents.

I shall always retain en route the classified documents/equipment and shall not open the package unless required by the Customs Authorities.

Upon arrival, I shall hand over the classified documents/equipment intended for the receiving company/organisation, against receipt, to the designated consignee.

(Place and date) (Signature of courier)

Witnessed by:

(Security Officer’s signature)

Appendix 9. INTERNATIONAL TRANSPORTATION PLAN

INTERNATIONAL TRANSPORTATION PLAN

[LETTERHEAD]

TRANSPORTATION PLAN
FOR THE MOVEMENT OF CLASSIFIED CONSIGNMENTS
(INSERT NAME OF PROGRAMME OR PROJECT)

1. INTRODUCTION

This transportation plan lists the procedures for the movement of classified *(insert Programme /Project / Contract name)* consignments between *(insert Programme Participants)*.

2. DESCRIPTION OF CLASSIFIED CONSIGNMENT

Provide a general description of the consignment to be moved. If necessary, a detailed, descriptive listing of items to be moved under this plan, including military nomenclature, may be appended to this plan as an annex. Include in this section a brief description as to where and under what circumstances transfer of custody will occur.

3. IDENTIFICATION OF AUTHORISED PARTICIPATING GOVERNMENT REPRESENTATIVES

This Section should identify by name, title and organisation, the authorised representatives of each Programme/Project participant who will receipt for and assume security responsibility for the classified consignment. Mailing addresses, telephone numbers, fax numbers and network addresses should be listed for each country's representatives.

4. DELIVERY POINTS

(a) Identify the delivery points for each participant (e.g., ports, railheads, airports, etc.) and how transfer is to be effected;

(b) describe the security arrangements that are required while the consignment is located at the delivery points; and

(c) specify any additional security arrangements, which may be required due to the unique nature of the movement or of a delivery point (e.g., an airport freight terminal or port receiving station).

5. IDENTIFICATION OF CARRIERS

Identify the commercial carriers, freight forwarders and transportation agents, where appropriate, that might be involved to include the level of security clearance and storage capability.

6. STORAGE/PROCESSING FACILITIES AND TRANSFER POINTS

(a) List, by participants, the storage or processing facilities and transfer points that will be used; and

(b) describe specific security arrangements necessary to ensure the protection of the classified consignment while it is located at the storage / processing facility or transfer point.

7. ROUTES

Specify in this section the routes for movements of the classified consignments under the plan. This should include each segment of the route from the initial point of movement to the ultimate destination including all border crossing. Routes should be detailed for each participant in the logical sequence of the shipment from point to point. If overnight stops are required, security arrangements for each stopping point should be specified. Contingency stop-over locations should also be identified as necessary.

8. PORT SECURITY AND CUSTOMS OFFICIALS

In this section, identify arrangements for dealing with customs and port security officials of each participant. The facility must verify that the courier has been provided with the necessary documentation and is aware of the rules necessary to comply with customs and security requirements. Prior co-ordination with customs and port security agencies may be required so that the Project/Programme movements will be recognised.

Procedures for handling custom searches and points of contact for verification of movements at the initial despatch points should also be included here.

9. COURIERS

When couriers are to be used, relevant provisions specified in Appendix 7 and 8 apply.

10. RECIPIENT RESPONSIBILITIES

Describe the responsibilities of each recipient to inventory the movement and to examine all documentation upon receipt of the movement and:

(a) notify the dispatcher of any deviation in routes or methods prescribed by this plan;

(b) notify the dispatcher of any discrepancies in the documentation or shortages in the shipment; and

(c) clearly state the requirement for recipients to promptly advise the NSA/DSA of the dispatcher of any known or suspected compromise of classified consignment or any other exigencies which may place the movement in jeopardy.

11. DETAILS OF CLASSIFIED MOVEMENTS

This section should include the following items:

(a) identification of dispatch assembly points;

(b) packaging requirements that conform to the national security rules of the Project/Programme participants. The requirements for dispatch documents seals, receipts, and storage and security containers should be explained. Any unique requirement of the Projects/Programme participants should also be stated; documentation required for the dispatch points;

(c) courier authorisation documentation and travel arrangements;

(d) procedures for locking, sealing, verifying and loading consignments. Describe procedures at the loading points, to include tally records, surveillance responsibilities and witnessing of the counting and loading arrangements;

(e) procedures for accessibility by courier to the shipment en route;

(f) procedures for unloading at destination, to include identification of recipients and procedures for change of custody, and receipt arrangements;

(g) emergency communication procedures. List appropriate telephone numbers and points of contact for notification in the event of emergency; and

(h) procedures for identifying each consignment and for providing details of each consignment (see Attachments); the notification should be transmitted no less than six working days prior to the movement of the classified consignment.

12. RETURN OF CLASSIFIED MATERIAL

This section should identify requirements for return of classified material to the manufacturer or sending country (e.g., warranty, repair, test and evaluation, etc.).

(a) Samples of these forms should be included, as appropriate, as enclosures to the plan as necessary.

(1) packing list;

(2) classified material receipts;

(3) bills of lading;

(4) export declaration;

(5) waybills;

(6) other nationally-required forms.

(b) NSAs/DSAs reserve their right to add additional measures in the course of establishing the Transportation Plan if required.

Appendix 10. NOTICE OF CLASSIFIED CONSIGNMENT

NOTICE OF CLASSIFIED CONSIGNMENT

NOTICE OF *(INSERT PROGRAMME/PROJECT NAME)*

CONSIGNMENT APPROVED TRANSPORTATION PLAN REFERENCE No.
(INSERT REFERENCE)

REPLY BEFORE: *(insert date)*

1. Consignor / consignee: *(include the name, telephone number and address of the person(s) responsible for the consignment at both locations)*.

2. Government Designated Personnel: *(include name, telephone number and address of releasing and receiving authorised representatives, as applicable)*.

3. Description of consignment:

   (a) contract or Tender Number;

   (b) export licence or other applicable export authorisation citation;

   (c) consignment description: *(describe items to be shipped and their classification);*

   (d) package description:

   - type of package (wood, cardboard, metal, etc.);
   - number of packages;
   - number of enclosed classified items in each package;
   - package dimensions/weight: *(include length, width, height and weight);*

   (e) indicate if package contains any hazardous material.

4. Routing of consignment:

   (a) date / time of departure;

   (b) date / estimated time of arrival;

   (c) routes to be used between point of origin, point of export, point of import and ultimate destination: *(identify specific transfer points; use codes that appear in transportation plan, if applicable)*;

   (d) method of transport for each portion of the shipment: *(include names and addresses of all carriers and flight, rail or ship numbers, as applicable)*;

   (e) freight forwarder s /transportation agents to be used: *(include name, telephone number, address of companies if not specified in transportation plan); (Note: Consignor must re-verify clearance and safeguarding capability of these entities prior to releasing shipments);*

(f) customs or port security contacts: *(list names and telephone numbers, if different from approved transportation plan procedures).*

5. Name(s) and identification of authorised courier.

ANNEX G. ACRONYMS

ABL	Allocated Baseline
ACCS	Air Command and Control System
AirC2IS	Air Command and Control Information Services
ALTBMD	Active Layered Theatre Missile Defence
Bi-SC AIS	Bi-Strategic Command Automated Information Services
BMC3I	Battle management, communications, command and control
BMD	Ballistic Missile Defence
BMGW	Broadcast Multicast Gateway
C2	Command and Control
CASE	Computer Aided Software Engineering
CBRN FS	Chemical Biological Radiological and Nuclear Functional Service
CBT	computer-based-training
CCB	Configuration Control Board
CDRL	Contract Data Requirement List
CFBLNet	Combined Federated Battle Laboratories Network
CI	Configuration Item
CIS	Communication Information System
CLIN	Contract Line Item Number
CM	Configuration management
CMDB	Configuration management Database
CoC	Certificate Of Conformity
COE	Consequence of Engagement
COI	Consequence of Intercept
CONI	Consequence of Non-Intercept
CONOPs	Concepts of Operation
COTS	Commercial off the shelf
CSA	Configuration Status Accounting

CSCI	Computer Software Configuration Item
DR	Deficiency Report
DTC	Document Type Code
ECP	Engineering Change Proposals
EDC	Effective Date of Contract
ERR	Engineering Release Record
ET	Ensemble Tests
ETEE	Education, Training, Exercise and Evaluation
EULA	End User Licence Agreement
FAT	Factory Acceptance Test
FBL	Functional Baseline
FCA	Functional Configuration Audit
FSA	Final System Acceptance
GFE	Government Furnished Equipment
HW	Hardware
ICC	Integrated Command and Control
Intel FS	Intelligence Functional Services
ILS	Integrated Logistics Support
IPT	Integrated Project Team
ITB	Integration Test Bed
LSID	Link 16 Situational Awareness Display
MSWAN	Mission Secret Wide Area Network
NCAGE	NATO Commercial and Government Entity
NCIA	NATO Communication Information Agency
NCOP	NATO Common Operational Picture
NCS	NATO Command Structure
NOR	NOTICE OF REVISION
NQAR	National Quality Assurance Representative
NSCM	NATO System Classification Number
NSWAN	NATO Secret Wide Area Network
OBL	Operational Baseline
OFS	Open Framework Services
OPS	Operational Services

OSS	Open Source Software
PMTP	Project Master Test Plan
PBL	Product Baseline
PCR	Project Checkpoint Reviews
PBS	Product
PFI	Purchaser Furnished Item
PM	Project Management
PMO	Project Management Office
PMP	Project Management Plan
PMR	Project Management Review
PMS	Project Master Schedule
PO	Program Office
POC	Point of Contact
PCA	Physical Configuration Audit
PSA	Provisional System Acceptance
QA	Quality Assurance
QAP	Quality Assurance Plan
QAR	Quality Assurance Report
QM	Quality Management
RACI	Responsible, Accountable, Consulted, Informed
RDP	Release and Deployment Plan
RFD	Requests for Deviation
RFW	Requests for Waiver
RMP	Risk Management Plan
RTM	Requirements traceability matrix
SAA	Security Accreditation Authority
SAT	System Acceptance Test
SDP	System Development Plan
SIT	System Integration Test
SOW	Statement of Work
SMD	System Maintenance Documentation
SRR	System Requirement Review
SRS	System Requirement Specifications

SSDD	System Subsystem Design Description
SSS	Schedule for Supplies and Services
STANAG	Standard Agreement
SVD	Software Version Description
SW	Software
TDD	Test Descriptions Documents
TMD	Theatre Missile Defence
TNA	Training Needs Analysis
TOPFAS	Tool for Operational Planning, Force Activation and Simulation
TRR	Test Readiness Review
TRM	Test Review Meeting
TVV	Testing, verification and validation
UAT	User Acceptance Test
UX	User Experience
VM	virtual machine
WBS	Work Breakdown Structure

Table 1 List of Acronym

ANNEX H – HOST ENVIRONMENT DECRIPTION

1.1 ITB OFS HOST ENVIRONMENT

The ITB OFS host environment is based on a virtualized environment which runs on the ITB own HW and SW Infrastructure. This infrastructure includes HW severs, clients, and network storage systems which enable to host the ITB OFS and most of the ITB PFX. The remaining ITB PFX are deployed on a dedicated HW Platforms such as for example the case of ACCS TMD1 and TDACS.

NCIA is currently procuring a near term upgrade of current ITB HW and SW Infrastructure to modernize current ITB Infrastructure and improve ITB performance and capabilities. This procurement will acquire for Core ITB and Ops ITB new servers and network storage systems based on the current Core ITB specification, built to the latest performance specifications and including 3D graphics. As a reference, the current Core ITB HW and SW infrastructure is described in section below.

1.2 Core ITB HOST ENVIRONMENT

The current Core ITB Infrastructure hosts the ITB Build 5 OFS and PFX and is composed of the following items.

- ***Virtualization/VDI***
  The Virtualization platform is based on VMWare ESXi (Ver. 6.0) / VSphere (Ver. 6.5) infrastructure designed to host Servers and a VMware Horizon solution to host Virtual Desktops. The ITB users have access to the ITB Capabilities through a standard WISE Thin Client VDI desktop from which they can open remote desktop sessions on a dedicated number of virtualized desktops where the specific ITB OFS and apps are installed (.e.g. Nautilus, Threat Injectors, Scenario Preparation etc.). The BL460 and the BL480 servers are dedicated to the VMWare infrastructure, one BL420 server is dedicated to run the main Domain Controller.

  HW Physical Servers:
  1 X HP C3000 enclosure
  1 X HP BL420C GEN 8, XEON, 1 CPU - 8 CORES, 256 GB RAM
  2 X HP BL460C GEN 8, XEON, 2 CPU - 12 CORES, 256 GB RAM
  1 X HP BL480/660 GEN10, XEON, 2 CPU - 16 CORES, 512 GBRAM

  Virtualized Machines:
  29 X Windows 10 Desktop
  9 X Linux (RHEL6, RHEL7, CentOS 4/5)
  3 X Solaris 10
  8 X Windows Server 2012/2016

- ***Storage***

HW: 2 X NetApp FAS 2220 NAS (Fibre Channel Over Ethernet, 4.9TB Usable space)
2 X NetApp FAS 2750 NAS (Fibre Channel Over Ethernet, 24TB Usable space)

- ***Networks***

The ITB lab is connected to the CFBLNet (RED Enclave) and the NSWAN. Ethernet connections are at 10GBps towards Blade servers and storage, 1 GB to the clients.

HW: L2/L3 Switching & Routing: Cisco based

- ***Video Distribution***

The ITB Video Distribution systems provides the capability to display each ITB Thin client video output to the local screens and to be redirected independently to each of the video output elements, either Projectors or Display Screens, located in the ITB lab.

- ***Voice Communication***

HW: CISCO Based. VOIP telephones on different networks and running ta different security classification.

- ***Current ITB OFS Deployment***

In current configuration, the ITB OFS are deployed as in the table below.

ITB B5 OFS	**Number of instances**
HLA RTI (SM)	**1**
DIS/HLA Bridge (SM)	**3**
Remote Site Manager (RS)	**1**
JREAP/SIMPLE Hub (OC)	**1**
Simulation Control (SC) Simulation Initialisation (SI)	**1**
Scenario Preparation (SP)	**1**
TBM Threat Generator (TI)	**1**
Air Breathing Threat (AB)	**1**
Data Collection Analysis Reporting (DC/AR)	**14**
2D	**1**
3D	**1**
Data Persistence and retrieval (ID)	**23**

NATO Communications and Information Agency
Agence OTAN d'information et de communication

<<Product>>

Baseline <<FBL, ABL or PBL>>

Engineering Release Record

ENGINEERING RELEASE RECORD (ERR)

ENGINEERING RELEASE RECORD (ERR)			
1. ERR No.	2. DATE	3. SHEET OF SHEETS	
4. ECP No.		5. EFFECTIVE DATE	

6. DATA RELEASED OR REVISED

NSCM (NCAGE) a.	DOCUMENT		REVISION		RELEASE		CHANGE		OTHER
	NUMBER b.	TITLE c.	LETTER d.	DATE e.	IR f.	NAR g.	CH h.	CAN i.	ECP NO.# j.

6. DATA RELEASED OR REVISED									
NSCM (NCAGE) a.	DOCUMENT		REVISION		RELEASE		CHANGE		OTHER
	NUMBER b.	TITLE c.	LETTER d.	DATE e.	IR f.	NAR g.	CH h.	CAN i.	ECP NO.# j.

CONTRACTOR APPROVAL	
7. SUBMITTED BY (Signature)	**8. APPROVED BY (Signature)**

End of Document

NOTICE OF REVISION (NOR)

1. ORIGINATOR NAME AND ADDRESS	2. DATE	3. NSCM (NCAGE)	4. NOR NO.	NOR Rev.

5. PURCHASER NAME	6. CONTRACT NO.	7. NSCM (NCAGE)	8. DOCUMENT NO.

9a. TITLE OF DOCUMENT	9b. REVISION (Current)	9b. REVISION (New)
	10. ECP NO.	

11. CONFIGURATION ITEM (OR SYSTEM) TO WHICH ECP APPLIES

a. Part Identification Number	b. CI Nomenclature

12. Related Changes (If not sufficient, use continuation sheets)

	Addition	CHANGE		
Page/Paragraph	Add	CH	CAN	Remark

13. THIS SECTION IS FOR PURCHASER USE ONLY

a. CHECK ONE		
☐ EXISTING DOCUMENT SUPPLEMENTED BY THIS NOR MAY BE USED IN MANUFACTURE.	☐ REVISED DOCUMENT MUST BE RECEIVED BEFORE MANUFACTURER MAY INCORPORATE THIS CHANGE.	☐ CUSTODIAN OF MASTER DOCUMENT SHALL MAKE ABOVE REVISION AND FURNISH REVISED DOCUMENT TO:
b. ☐ APPROVED ☐ DISAPPROVED	PURCHASER SIGNATURE	DATE:

14. NAME OF ORGANISATION ACCOMPLISHING REVISION	15. REVISION COMPLETED Signature Date

NATO Communications and Information Agency
Agence OTAN d'information et de communication

<<Product>>

Release <<Release>>

Software Version Description

Released by
NATO Programming Centre

Release Notice

<<Release Notice>>

Authority Page

<<Product Name>>

Software Version Description

Version <<document version>> <<Date>>

Authored by:

<<Name Surname>>
Configuration Manager

Date: <<Date>>

Approved for Release by:

<<Name Surname>>
<<Grade>>
Chief Service Transition Branch

Date: <<Date>>

Document Update History

Release : <<Product Release>>

Document Version : <<Version>>

POW Objective	Title	Pages Affected
<<POW Id>>	<<POW Title>>	<<Pages>>

Table of Contents

List of Tables

1 Scope

Item Text

1.1 Product Overview

Item Text

<<Product description → Maybe Excerpt from the Product Catalogue>>

1.2 Document Overview

Item Text

2 Relevant Documents

Table 1 lists documents relevant to this SVD.

Table 1 – Relevant Documents

	Ref.	Issue	Title
A.	ACO Directive 70-001	<<Version>>	ACO Security Directive
B.	<<Document>>	<<Version>>	<<Description>>

3 Release Description

3.1 Full Identification

System Name:	<<optional if applicable>>
Product Name:	AutoFill
Short Name:	AutoFill
Version:	AutoFill
Release Type:	<<ReleaseType>>
Production Baseline:	BP_XXXX
Production Date:	<<Date>>

3.2 Hardware Requirements

The minimum recommended hardware requirements are detailed in Table 4.

3.3 Interoperability

3.3.1 Software Compatibility

This baseline has been verified to function correctly with the operating systems specified in Table 2.

Table 2 - Operating Systems Compatibility List

Software Item Name	Version

In addition, this baseline has been verified to be compatible with the air defence software and systems listed in Table 3.

Table 3 - Air Defence Software Compatibility List

Software Item Name	Version

3.3.2 Hardware Compatibility

This baseline version has been verified on a number of hardware/operating system combinations. The configurations are detailed in Table 4 and can be considered as being the minimum requirements to run this baseline.

Table 4 - Hardware/Operating System Compatibility Overview

Hardware Platform	Operating System

3.4 Release History

Table 5 lists all currently supported versions of this product.

Table 5 - Supported Product Versions

Product Name	Version	Release Date
<<Product>>	Current Version	MMM YYYY
<<Product>>	Current Version - 1	MMM YYYY
<<Product>>	Current Version - 2	MMM YYYY

4 Change Description

4.1 Significant Changes Implemented in this Release

This part should describe the biggest impacts to the user since the last release was published. For example changes in the minimal system requirements or in the way of working. It is also possible to point to another document with the detailed description (e.g. SUM, SIP).

4.2 Implemented Engineering Change Proposals (ECP)

The ECPs listed in Table 6 and Table 7 are implemented in this baseline release.

Table 6 – Class I ECPs (Enhancements) Implemented in this Release

ECP Number	Title

Table 7 – Class II ECPs (Corrections) Implemented in this Release

ECP Number	Title

4.3 System Update Reports (SURs)

All Software Update Reports related to the implemented ECP are listed in Annex A

4.4 Known Issues

All known matters that could not be resolved with this release are listed in Annex B

5 Product Description

5.1 Delivered Media

The <<ProdShortName>> <<X.Y.Z>> release is distributed with the set of media identified in Table 8.

Table 8 – List of Media Delivered with this Release

Media Label Identification	Version	Creation Date	Media Type	Classification
<<Media Title>>	<<X.Y.Z>>	MMM YYYY	DVD	NU
<<Media Title>>	n/a	MMM YYYY	CD	NU

5.2 Software Items

All high level Software Items included in this release are listed in Annex C .

5.3 Delivered Documentation

All Documents listed in Table 9 can be found on the media delivered with this release.

Table 9 – List of Documents Delivered with this Release

Identification / Title	File Name	Version	Date	Classification

5.4 Related Documentation

The following documents have been updated in respect of this release and are available upon request via the NPC Service Desk.

Table 10 – List of Documents Delivered with this Release

Identification / Title	File Name	Version	Date	Classification

Annex A - System Update Reports (SUR)

ECP DATA	System Update Report (SUR)		
Date Form Raised			
Change Type			
ECP Number			
Short Title			
Applicable To Sites			
BRIEF DESCRIPTION			
Problem/Background			
Solution			
USER IMPACT			
CM VERIFICATION OF SUR DATA			
Date:		Name:	

Annex B - Known Issues

Number	Severity	Title	Description	Workaround
123	Low	<<Issue Title>>	<<Issue Description>>	

Annex C - High Level Software Items

<<Media Title>>

File Name	Identification / Title	Version	Date	Class

<<Media Title>>

File Name	Identification / Title	Version	Date	Class

Annex D - Abbreviations

Table 11 – List of Abbreviations

Abbreviation	Description
ACO	Allied Command Operations
AEGIS	Airborne Early Warning Ground Environment Integration Segment
AOI	Area of Operational Interest
ATA	Air Target Area
BTA	Baseline Technical Assessment
CDE	Common Desktop Environment
CI	Configuration Item
CIS	Communication and Information Systems
CMO	Configuration Management Office
CRC	Control and Reporting Centre
CSD	Customer Service Desk
CSI	CRC System Interface
DP	Display Plugin
DVD	Digital Versatile Disc
ECP	Engineering Change Proposal
GUI	Graphical User Interface
HMI	Human-Machine Interface
ICAO	International Civil Aviation Organization
ICM	Inter Console Marker
IDO	Identification Officer
MRP	Multi-reference Point
NADGE	NATO Air Defence Ground Environment
NATO	North Atlantic Treaty Organization
NCIA	NATO Communications and Information Agency
NGCS	NATO Global Communications System
NISP	NPC Integrated Solaris Package
NOT	NPC Observation Tool
NPC	NATO Programming Centre
NPE	Null Pointer Exception
NU	NATO UNCLASSIFIED
T&E	Test and Evaluation
PDF	Portable Document Format

Abbreviation	Description
PDG	Preset Data Grouping
PMP	Project Management Plan
POW	Programme of Work
PP	Project Plan
PPI	Plan Position Indicator
SAD	Software Architecture Document
SIF	Selective Identification Feature
SIP	Software Installation Plan
SRS	Software Requirements Specification
STP	Software Test Plan
STR	Software Test Report
SUR	System Update Report
SVD	Software Version Description
TCT	Tell Criteria Tote
VOI	Voice Over IP
WAN	Wide Area Network

REQUEST FOR DEVIATION (RFD)/REQUEST FOR WAIVER (RFW)

1. ORIGINATOR NAME AND ADDRESS (TYPED)				2. NCAGE (fr. NSCM)	3. ☐ DEVIATION ☐ WAIVER
4. PURCHASER NAME				5. CONTRACT NO.	6. DATE
6. DESIGNATION FOR DEVIATION/WAIVER				8. BASELINE AFFECTED ☐ FBL ☐ ABL ☐ PBL	9. OTHER SYSTEMS OR CONFIGURATION ITEMS AFFECTED ☐ NO ☐ YES
a. MODEL/TYPE	b. NCAGE (NSCM)	c. SYS DESIG.	d. DEV/WAIVER NO.		
10. TITLE OF DEVIATION/WAIVER					
11. CONTRACT NO. AND LINE ITEM				12. PROCURING CONTRACTING OFFICER CODE	TELEPHONE
13. CONFIGURATION ITEM NOMENCLATURE					
14. NAME OF LOWEST PART/ASSEMBLY AFFECTED				15. PART NO. OR TYPE DESIGNATION None	
16. LOT NO.				17. QTY N/A	18. RECURRING DEVIATION/WAIVER ☐ YES ☐ NO
19. EFFECT ON COST/PRICE				20. EFFECT ON DELIVERY SCHEDULE None	
21. EFFECT ON INTEGRATED LOGISTICS SUPPORT, INTERFACE OR SOFTWARE					
22. DESCRIPTION OF DEVIATION/WAIVER					
23. NEED FOR DEVIATION/WAIVER					
24. CORRECTIVE ACTION TAKEN					
25. SERIAL NUMBER(S) AFFECTED None					
26. SUBMITTING ACTIVITY AUTHORISED SIGNATURE				27. TITLE Contract Management Department	
28. PURCHASER APPROVAL/DISAPPROVAL ☐ APPROVED ☐ DISAPPROVED				29. PURCHASER SIGNATURE AND DATE OF APPROVAL	