Acquisition Directorate
Boulevard Leopold III B-1110
Brussels, Belgium

NCIA/ACQ/2023/06756
31 March 2023

To : Bidders List and Distribution List

Subject : **Invitation For Bid IFB-CO-115791-DEMETER; Amendment 2**

References :
A. AC/4-D/2261(1996 Edition), Procedures for International Competitive Bidding
B. AC/4-D(2008)0002-REV2, International Competitive Bidding Using Best Value Evaluation Methodology, dated 15 July 2015
C. NCI Agency NOI NCIA/ACQ/2022/07326, dated 19 December 2022
D. NCI Agency IFB NCIA/ACQ/2023/06536, dated 03 March 2023
E. NCI Agency IFB Amendment 1; NCIA/ACQ/2023/06695 dated 17 March 2023

Dear Prospective Bidders,

1. The purpose of this Amendment 2 is to:

   a). Publish Release 1 of IFB Bidders' questions and NCI Agency responses,
   b). Deliver unclassified documents referenced in SOW and SRS.

2. Responses to Questions with the status Under Consideration will be provided by the Purchaser through the forthcoming Amendment 3.

3. All future Requests for Clarification (RfC)shall arrive not later than fourteen (14) calendar days before the established Bid Closing Date. Any clarifications received after that date will be answered at the discretion of NCI Agency Additional RfC may be responded to, however will not extend the Bid Closing Date. This decision shall not be a subject for dispute.

4. The closing time for submission of bids in response to this Invitation For Bid (IFB) remains Monday**, 15 May 2023**, 14:00 Hours (Central European Time (CET)).

5. All NATO Unclassified documents referenced in SOW and SRS are hereby delivered in eight (8) separate emails.This letter contains an itemized list of NU Unclassified documents provided in this Amendment 2.

NATO Communications and Information Agency
Agence OTAN d'information et de communication
Avenue du Bourget 140
1110 Brussels, Belgium
www.ncia.nato.int

Reference source	Document Name	Delivred
SOW	[ACMP-2009-SRD-41] Examples of Configuration Management Plan Requirements, Ed.A V1, Mar 2017	Email 1 of 8
SOW	[ACMP-2100] The Core Set of Configuration Management Contractual Requirements, Ed.A V2, Mar 2017	Email 1 of 8
SPW	[AD-070-001] ACO Directive 070-001 Allied Command Operations Security Directive, Dec 2021	Email 1 of 8
SOW	[AI-16.31.03] NCIA - Agency Instruction 16.31.03, Requirements for the preparation of IPSP, Sep 2022	Email 1 of 8
SOW	[ALP-10] NATO Guidance on Integrated Logistics Support for Multinational Armament Programmes, Ed.C V1, 2017	Email 1 of 8
SOW	[AQAP-2070] NATO Mutual Government Quality Assurance (GQA)	Email 1 of 8
SOW	[AQAP-2105] NATO Requirements for Quality Plans, Ed.C V1, Jan 2019	Email 1 of 8
SOW	[AQAP-2110] NATO Quality Assurance Requirements for Design, Development and Production, Ed.D V1, Jun 2016	Email 1 of 8
SOW	[AQAP-2210] NATO Supplementary SQA Requirements to AQAP-2110 or AQAP-2310, Ed.A V2, Sep 2015	Email 1 of 8
SOW	[AQAP-4107] Mutual Acceptance of Government Quality Assurance, Edition A, Version 2, Nov 2018	Email 1 of 8
SOW	[ASOP-07.01.25] NCI Academy Standard Operating Procedure - Grading and Assessment, May 2020	Email 1 of 8
SOW	[NATO-Bi-SC-DIR-075-007] NATO Bi-SC Education and Individual Training Directive (EITD) 075-007, Sep 2015	Email 1 of 8
SOW	[NCIA-AD-06.00.16] NCIA - Agency Directive 06.00.16, Configuration Management, Feb 2020	Email 2 of 8
SOW	[NCIA-AI-23.02] NCIA - Agency Instruction 23.02, Deployment Management Planning, Oct 2019	Email 2 of 8
SOW	[NCIA-AI-TECH-06.03.01] NCIA - Agency Instruction 06.03.01, Identification of Software Assets, Jun 2016	Email 2 of 8
SOW	[NCIA-SOP-06.03.05] NCIA - Agency Standard Operating Procedure 06.03.05, Software Patch Management, Oct 2020	Email 2 of 8
SOW	[NCIA-SOP-23.01] NCIA - Agency Standard Operating Procedure 23.01, Enterprise IT Change Management, Mar 2020	Email 2 of 8
SOW	[STANAG-4107] Mutual Acceptance of Government Quality Assurance	Email 2 of 8
SOW	[STANAG-4427] Edition 3 - Configuration Management in System Life Cycle Management	Email 2 of 8
SRS	LOGFAS ICD ANNEX A	Email 3 of 8
SRS	(NU) AC322-D(2019)0034 (INV) Consultation, Command and Control Board (C3B) C3 Taxonomy BL 3.1	Email 4 of 8
SRS	(NU) AC322-D(2019)0038 (INV) Directive for the Security of Web Applications	Email 4 of 8
SRS	(NU) AD 80-84 NATO Recognized Ground Picture	Email 4 of 8
SRS	(NU) C-M (2002) 49 Security within the NATO	Email 4 of 8

SRS	(NU) C-M (2015) 0041 Alliance Consultation, Command, And Control Policy	Email 4 of 8
SRS	(NU) CO-115718-I2BE INTEL-FS Spiral 2 - Information Model - Data Dictionary Tabular	Email 5 of 8
SRS	(NU) MC 0593-1	Email 6 of 8
SRS	(NU) MC 0640	Email 7 of 8
SRS	(NU) PO(2021)0360 Data Exploitation Framework Policy	Email 8 of 8
SRS	(NU) STANAG 4774 Confidentiality Metadata Labelling Syntax - Edition A - Version 1	Email 8 of 8
SRS	(NU) STANAG 4778.2 Profiles for Binding Metadata to a Data Object Edition A - Version 1 December 2020	Email 8 of 8
SOW	[ASD-AIA-SX000i] International Specification for Integrated Product Support (IPS), Issue No.3.0, Apr 2021 https://www.sx000i.org/docs/SX000i%20Issue%203.0.pdf	Email 1 of 8
SOW	[ASD-S3000L] International Procedure Specification for Logistic Support Analysis (LSA), Issue No.2.0, Apr 2021 https://www.s3000l.org/docs/S3000L%20Issue%202.0.pdf	Email 1 of 8
SOW	[ISO/IEC/IEEE-29119] International Standard for Software Testing, 2022 https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html	Email 1 of 8
SOW	[ISO/IEC/IEEE-29148] International Standard for Systems and software engineering – Life cycle processes – Requirements engineering, 2011 https://www.iso.org/standard/72089.html	Email 1 of 8
SOW	[ISO-9000:2015] Quality management systems – Fundamentals and vocabulary https://www.iso.org/standard/45481.html	Email 1 of 8

6. Prospective Bidders are advised that the NCI Agency reserves the right to cancel this IFB at any time in its entirety and bears no liability for bid preparation costs incurred by firms or any other collateral costs if bid cancellation occurs.

7. This IFB remains the property of the NCI Agency and shall be protected in accordance with the applicable national security regulations.

8. The NCI Agency point of contact for all information concerning this IFB is Mr. Radu Munteanu, Contracting Officer, who may be reached at CO115791DEMETER@ncia.nato.int.

FOR THE CHIEF OF ACQUISITION:

Radu Munteanu
Digitally signed by Radu Munteanu
Date: 2023.03.31 17:23:05 +02'00'

Radu Munteanu
Contracting Officer

Attachments:

A) Responses to Clarification Requests, Release Number 1
B) Unclassified documents referenced in SOW and SRS

Distribution List

All Nominated Prospective Bidders

NATO Delegations (Attn: Infrastructure Adviser):

- Albania
- Belgium
- Bulgaria
- Canada
- Croatia
- Czech Republic
- Denmark
- Estonia
- France
- Germany
- Greece
- Hungary
- Iceland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Montenegro
- The Netherlands
- North Macedonia
- Norway
- Poland
- Portugal
- Romania
- Slovakia
- Slovenia
- Spain
- Turkey
- United Kingdom
- United States

NATO HQ

- NATO Office of Resources (NOR)
  - CIS and Cyber Capabilities Branch (CCC) Branch Head
  - NOR Secretariat Section (RPPB, IC, BC)

NCI Agency – NATEXs

NCI Agency

ACQ Chief of Acquisition – Ms. J Uptton
ACQ Deputy Chief of Acquisition – Mr. A Vitry

ACQ Restricted Contract Award Board Administrator – Mr N Rego
ACQ Principal Contracting Officer - Mr JL Guellec
ACQ Contracting Officer – Mr. R Munteanu
Chief C2 Centre – Dr P. Howland
Project Manager C2 SC – Mr. W Leeming
Legal Office
Registry

Attachment 1: Responses to Clarification Questions, Release Number 1

#	RFP Source Document	Offeror's Question	Purchaser Clarification
1	SRS-001, SRS-002	Could the NCI Agency provide for Bidder with the following reference documents, listed in the document IFB-CO-115791 BOOK II - PART IV SOW Annex A SYSTEM REQUIREMENTS SPECIFICATION (SRS)? The following documents are necessary for the proper preparation of the offer: • [NREF-11][AC/322-D(2019) 0038 (INV) CIS Security Technical and Implementation Directive for the Security of Web Applications.] • [AC_322-D_0048-REV3][Technical and Implementation Directive on CIS Security] • [R-ICD-AT-06.02.14-Map][Agency Technical Instruction AI Tech 06.02.14 Service Interface Profile for Geospatial Services - Map Rendering Service 16 September 2016] • [R-ICD-Intel-FS-DM][CO-115718-I2BE, INTEL-FS Spiral 2 NAF 4.0 L7 Information Model Data Dictionary - All Entities Nov 8, 2022 4:58 PM] • [R-ICD-JOCWatch][JOCWatch 4.1 Interface Control Document Oct 2022] • [R-ICD-FasInterop][TOPFAS/LOGFAS ADL-FPH ORBAT Schemas version 2022.7] • [R-ICD-Namis][Interface Control Document NAMIS v3.4.16 version 1.0 date 21/11/2018] • [R-ICD-NCOP2][Interface Control Document NCOP2 ICD 7 June 2022] • [R-ICD-TOPFAS-DM][TOPFAS Increment-2 Software Design Specification Annex 1: Database Model (Desktop) 8/5/2020] • [R-ICD-TOPFAS-ICD][TOPFAS Increment-2 Software Design Specification Annex 3: Interface Control Document (Desktop) 15/09/2020] • [R-ICD-SOA_IdM][CO-14176-SOA-IDM Service Oriented Architecture (SOA) and Identity Management Platform (IdM) Wave I Interface Control Document (ICD) Doc. Version: 15.0 Date: 08/06/2021] • [R-ICD-TOPFAS-Excel][Empty Plan Collecting Sheet Months All Collectors Dated December 2022] • [R-ICD-LOGFAS][LOGFAS INTERFACE CONTROL DOCUMENT 30-Jan-23 Version 8.0.0] • [CM (2007)0118][NATO Information Management Policy (NMIP)] • [C-M (2011)0042][NATO Policy on Cyber Defence] • [AC/35-D/2004][Primary Directive on INFOSEC, NATO Security Policy supporting directive] • [C-(2008)0113(INV)][NATO Information Assurance Policy] • [C-M(2007)0118][NATO Information Management Policy (NMIP)] • [R-ATP322][Command and Control of Allied Land Forces] • [R-TID-CISSec][NATO AC/322-D/0048 - Technical and Implementation Directive on CIS Security.] • [Ref-CCat][NATO Communications and Information Agency Costed Customer Services Catalogue v7.1 2023Service Definitions] • IEG-C [R-ICD-IEGC] Interface Control Document IEG-C • [NREF-JOEL]AC35-D(2002)-DIRECTIVE on the SECURITY of INFORMATION-REV3	These requested documents have been transmitted on 17 & 18 March 2023: - [AC_322-D_0048-REV3][Technical and Implementation Directive on CIS Security] - [R-ICD-AT-06.02.14-Map][Agency Technical Instruction AI Tech 06.02.14 Service Interface Profile for Geospatial Services - Map Rendering Service 16 September 2016] - [R-ICD-JOCWatch][JOCWatch 4.1 Interface Control Document Oct 2022] - [R-ICD-Namis][Interface Control Document NAMIS v3.4.16 version 1.0 date 21/11/2018] - [R-ICD-NCOP2][Interface Control Document NCOP2 ICD 7 June 2022] - [R-ICD-TOPFAS-DM][TOPFAS Increment-2 Software Design Specification Annex 1: Database Model (Desktop) 8/5/2020] - [R-ICD-TOPFAS-ICD][TOPFAS Increment-2 Software Design Specification Annex 3: Interface Control Document (Desktop) 15/09/2020] - [R-ICD-TOPFAS-Excel][Empty Plan Collecting Sheet Months All Collectors Dated December 2022] - [R-ICD-LOGFAS][LOGFAS INTERFACE CONTROL DOCUMENT 30-Jan-23 Version 8.0.0] - [CM (2007)0118][NATO Information Management Policy (NMIP)] - [AC/35-D/2004][Primary Directive on INFOSEC, NATO Security Policy supporting directive] - [C-(2008)0113(INV)][NATO Information Assurance Policy] - [C-M(2007)0118][NATO Information Management Policy (NMIP)] - [R-ATP322][Command and Control of Allied Land Forces] - [R-TID-CISSec][NATO AC/322-D/0048 - Technical and Implementation Directive on CIS Security.] - [Ref-CCat][NATO Communications and Information Agency Costed Customer Services Catalogue v7.1 2023Service Definitions] The remaining documents requested will be transmitted, except for: - [R-ICD-SOA_IdM]: SOA-IdM documentation will be provided as soon as possible. Note that STANAG 4774 and 4778.2 (included in document delivery) instead of [R-ICD-IEGC] shall be used.
2	SRS-034	What are the technical requirements regarding the method of signing the ordering document? How are "authoritative data sources" determined?	There are no specific technical requirements for signing the order document. The question about authoritative data sources is not relevant for this requirement.
3	SRS-110	How will the test confirming compliance with this requirement be carried out?	Refer to Bidding Instructions section 4.8 for the Post Evaluation Test Drive
4	SRS-028	What communication interface should be used to transfer operational data for OPLAN from TOPFAS?	Information provided in ICD
5	SRS-117	What communication interface should be used to deliver the Situation Update to TOPFAS?	Information provided in ICD
6	SRS-140	What is the purpose of micro environments? What functionalities should DEMETER provide to meet this requirement?	Under Consideration
7	SRS-152	What is the expected manner and scope of verification of compliance with this requirement through demonstration?	Under Consideration
8	SRS-152	Whether a demonstration in an environment with equivalent parameters is allowed?	Under Consideration
9	SRS-152	Could the NCI Agency provide the Bidder with the NATO DCIS nodes infrastructure (current and planned) specification? The document is necessary for the proper preparation of the offer.	Under Consideration
10	SRS-154	What is the expected manner and scope of verification of compliance with this requirement through demonstration?	Under Consideration
11	SRS-154	Whether a demonstration in an environment with equivalent parameters is allowed?	Under Consideration
12	SRS-154	Could the NCI Agency provide the Bidder with the specification of NATO's Mission Information Room (MIR) infrastructure? The document is necessary for the proper preparation of the offer.	Under Consideration
13	SOW-242	Could the NCI Agency provide the Bidder with document NATO-Bi-SC-DIR-075-007? The document is necessary for the proper preparation of the offer.	This document will be transmitted.
14	SOW-289	What product is intended for the preparation of online training materials in accordance with the Sharable Content Object Reference Model (SCORM) Edition 2004? Will the NCI Agency provide the Bidder with a license for such software for the time of the training materials preparation?	SOW-289 targets any form of eLearning materials developed for DEMETER. eLearning is defined in the SOW as "Self-paced online learning, covering a complete or partial course". This statement dictates compliancy with the Sharable Content Object Reference Model (SCORM) Edition 2004. There is no licence required for SCORM compliancy. Any eLearning development tool in the market can publish SCORM 2004 compliant content. For the development of the eLearning content, NCI Agency will not provide licence for the development tools used by the Bidder.
15	164	Could the NCI Agency provide the Bidder with a document "[ASD-AIA-SX000i] International Specification for Integrated Product Support (IPS), Issue No.3.0, Apr 2021" and "[ASD-S3000L] International Procedure Specification for Logistic Support Analysis (LSA), Issue No.2.0, Apr 2021"? The document is necessary for the proper preparation of the offer.	These documents are available on the internet: - https://www.sx000i.org/docs/SX000i%20Issue%203.0.pdf - https://www.s3000l.org/docs/S3000L%20Issue%202.0.pdf
16	SOW-349	Could the NCI Agency provide the Bidder with the document "NATO Guidance on Integrated Logistics Support for Multinational Armament Programs, Ed.C V1, 2017"? The document is necessary for the proper preparation of the offer.	This document will be transmitted.
17	SOW 1.4.3 [24]	What is the preferred scheduled date for PSA WP-3	Refer to SOW figure 1.2 and Bidding sheets: Payment Schedule
18	SOW-313	Does the Purchaser require the Contractor to perform design and build activities to implement adaptation features modifying the selected integration platform or does the Purchaser require the Contractor to implement integration features only into Contractor's product?	The Contractor shall design and build interoperability adaptations on an NCI Agency approved integration platform.
19	SOW-002	In [SOW-002] PSA for WP1 is described as EDC + 11 months. In Annex A – Bidding Sheets, CLIN 1.6.2 (Installation and activation for Work Package 1 / PSA") PSA is described as EDC + 9 months. What is the required completion date for Work Package 1 PSA?	As stated in figure 1.2 of the SOW, PSA for WP1 shall be EDC + 11 months. SSS CLIN 1.6.2 will be updated accordingly.

20	SOW [23], Book I 3.5.7.5.1	Does the Purchaser allow or require the Contractors to implement features, stated in SRS, that are currently unavailable or partially available in the COTS solution to be delivered in the next upcoming releases? Is it possible to deliver those functionalities within WP3?	All features are to be delivered by PSA of WP2.
21	SOW-011	Does the Contractors' personnel (software developers, testers, administrative staff etc.) assigned to the project performing activities in the Contractor's office that do not require access to classified information and will not perform work in NATO premises, need to have NATO SECRET security clearance?	Contractor/Sub-contractor's personnel, including freelance consultants and interpreters, or any other type of freelance personnel or self-employed service providers who carry out works on NATO premises or Contractor's facilities in connection with a classified NATO programme/project or any other type of NATO contract requiring access to information classified NC or above shall hold a PSC at the requisite level and, if required by national laws and regulations, an appropriate FSC. This means that, as the contract is at NC or above then the Contractor personnel in question would in fact need to hold a PSC at the appropriate level. The company would also need a Facility Secuity Clearance (FSC).
22	SOW-127	Which test management and automation tools are used by the Purchaser? Please provide ICD documentation.	JIRA with the Zephyr plugin for test management and Azure automation tools. No ICD provided as part of these tools.
23	SOW-129	Which requirements coverage supporting tools and defect management tools are used by the Purchaser? Please provide ICD documentation.	Requirements management: IBM DOORS. Defect management: JIRA and Azure tooling. No ICD provided as part of these tools.
24	BOOK II - PART IV SOW, 9 - References	Could the contracting authority provide the following reference documents, which the contracting authority refers to in the document IFB-CO-115791 BOOK II - PART IV SOW? The following documents are necessary for the proper preparation of the offer: • [AD-070-001] ACO Directive 070-001 Allied Command Operations Security Directive, Dec 2021 • [AI-16.31.03] NCIA - Agency Instruction 16.31.03, Requirements for the preparation of IPSP, Sep 2022 • [ALP-10] NATO Guidance on Integrated Logistics Support for Multinational Armament Programs, Ed.C V1, 2017 • [ASD-AIA-SX000i] International Specification for Integrated Product Support (IPS), Issue No.3.0, Apr 2021 • [ASD-S3000L] International Procedure Specification for Logistic Support Analysis (LSA), Issue No.2.0, Apr 2021 • [ASOP-07.01.25] NCI Academy Standard Operating Procedure - Grading and Assessment, May 2020 • [NATO-Bi-SC-DIR-075-007] NATO Bi-SC Education and Individual Training Directive (E&ITD) 075-007, Sep 2015 • [NCIA-AD-06.00.16] NCIA - Agency Directive 06.00.16, Configuration Management, Feb 2020 • [NCIA-AI-23.02] NCIA - Agency Instruction 23.02, Deployment Management Planning, Oct 2019 • [NCIA-AI-TECH-06.03.01] NCIA - Agency Instruction 06.03.01, Identification of Software Assets, Jun 2016 • [NCIA-SOP-06.03.05] NCIA – Agency Standard Operating Procedure 06.03.05, Software Patch Management, Oct 2020 • [NCIA-SOP-23.01] NCIA – Agency Standard Operating Procedure 23.01, Enterprise IT Change Management, Mar 2020 • [R-ICD-NIRIS] Track Store Open API interface – original version to be provided • [SOA-IdM] SOA-IDM Service Oriented Architecture (SOA) and Identity Management (IdM) Platform - Wave 1 - Interface Control Document (ICD) V15.0, Jun 2021 - System Design Specification (SDS) V9.3, May 2021 • [STANAG-4427] Edition 3 - Configuration Management in System Life Cycle Management • [XSD-LC2IS] Interface Control Document (ICD) for LC2IS Inc 2 Contract no CO-14463-LC2IS F0057 62794795 558 Rev M - Annex E LC2IS Inc 2 XML Schema Definition	All documents requested will be transmitted, except for: - [R-ICD-NIRIS]: will be provided as soon as possible. - [SOA_IdM]: SOA-IdM documentation will be provided as soon as possible. - [XSD-LC2IS]: this document will be provided as soon as possible. These documents are available on the internet: - [ASD-AIA-SX000i]: https://www.sx000i.org/docs/SX000i%20Issue%203.0.pdf - [ASD-S3000L]: https://www.s3000l.org/docs/S3000L%20Issue%202.0.pdf
25	SOW Annex-A, p.28, SRS-139	The requirement contains that "DEMETER system intrinsic availability is greater than 99.5%." Intrinsic (theoretical) availability will be calculated for DEMETER's software architecture/CSCIs only. There will be no models generated, i.e. no diagrams like RBD for hardware, but assessment on software maturity will be made after getting diminishing software error data, during unit tests and integration tests. For third-party software this value will be taken as 100%. Is this assumption correct?	Yes, the claim shall be supported by collected data.
26	SOW Annex-A, p.45, SRS-256	The requirement contains that "DEMETER exhibits a mean-timebetween- failure (MTBF) characteristic of less than 3.65 hours per month..." Could you explicitly elaborate on, what is intended here? What is the equivalence of this specific MTBF target value?	Application shall have redundancy to be able to recover from failures within specified timeline.
27	SOW Annex-A, p.58, SRS-322 and SRS-323	In order to evaluate our compliance, we need detailed information about the following content; • Metadata format or standard used in NIP • The interface standards for the NIP	Under Consideration
28	SOW, p.59, SOW-366 p.62, SOW-383 p.64, SOW-395	The times for the provision of workarounds (two business days) and the defect fixing (ten days) for critical defects mentioned in SOW-366 seems to be conflicting with the times mentioned in SOW-383/SOW-395 (eight business hours for workarounds, and four business days for fixed solution). Could you explicitly elaborate on these requirements?	SOW-366 in the Maintenance and Support Concept is a typo. And will be updated in a forthcoming amendment. The service level to be respected during Warranty and (Optional Maintenance and Support) Post-Warranty periods are the SOW-383 and SOW-395.
29	SOW, p.62, SOW-384	The last sentence of SOW-384 states that "…the Contractor's response time at Purchaser site shall be within two business days from the moment of Purchaser notification. Our understanding is that this "2-business days of response time" is not included in the defect fixing time mentioned in SOW- 366, SOW-383 and SOW-395? Could you explicitly elaborate on this?	As explicitly written in SOW-384 and SOW-396: The Contractor shall integrate the provision of on-site service support within its maintenance services to be provided off-site from the Contractor's facilities, or on-site at the Purchaser facilities as required in case the issue cannot be resolved remotely or to support warranty releases and deployment and hand-over thereof. In case on-site support provision at the Purchaser facilities is required, the Contractor's response time at Purchaser site shall be within two business days from the moment of Purchaser notification. The 2 days are additional to the 4 business days requested in the SOW-383/SOW-395 for the patch release. Moreover the 2 additional days shall start: 1. If deemed necessary by Purchaser to accomplish the deployment 2. After the Purchaser notification of request for on-site support
30	SOW Annex-A, p.54, SRS-301	Is the Service Catalogue provided in [Ref-ATP-A2SL]? If not provided, could you please define Service Catalogue.	Under Consideration

31		Could you please provide guidance on obtaining the reference documents listed in ANNEX E of the bid package from the NCIA, or suggest an appropriate alternative way? Reference ID Reference Document Details R-ICD-AT-06.02.14-Map Agency Technical Instruction AI Tech 06.02.14 Service Interface Profile for Geospatial Services - Map Rendering Service 16 September 2016 R-ICD-Intel-FS-DM CO-115718-I2BE, INTEL-FS Spiral 2 NAF 4.0 L7 Information Model Data Dictionary - All Entities Nov 8, 2022 4:58 PM R-ICD-JOCWatch JOCWatch 4.1 Interface Control Document Oct 2022 R-ICD-FasInterop TOPFAS/LOGFAS ADL-FPH ORBAT Scemas version 2022.7 R-ICD-Namis Interface Control Document NAMIS v3.4.16 version 1.0 date 21/11/2018 R-ICD-NCOP2 Interface Control Document NCOP2 ICD 7 June 2022 R-ICD-TOPFAS-DM TOPFAS Increment-2 Software Design Specification Annex 1: Database Model (Desktop) 8/5/2020 R-ICD-TOPFAS-ICD TOPFAS Increment-2 Software Design Specification Annex 3: Interface Control Document (Desktop) 15/09/2020 R-ICD-SOA_IdM CO-14176-SOA-IDM Service Oriented Architecture (SOA) and Identity Management Platform (IdM) Wave I Interface Control Document (ICD) Doc. Version: 15.0 Date: 08/06/2021 R-ICD-TOPFAS-Excel Empty Plan Collecting Sheet Months All Collectors Dated December 2022 R-ICD-LOGFAS LOGFAS INTERFACE CONTROL DOCUMENT 30-Jan-23 Version 8.0.0 C-M (2011)0042 NATO Policy on Cyber Defence (Restricted) Ref-Ccat NATO Communications and Information Agency Costed Customer Services Catalogue v7.1 2023 Service Definitions Ref-DEFP PO(2021)0360 Data Exploitation Framework Policy R-ICD-IEGC To be delivered (related documents send STANAG 4774, 4778) R-RGP AD 80-84 NATO Recognized Ground Picture R-4778.2-BindProf STANAG 4778.2 Profiles for Binding Metadata to a Data Object Edition A - Version 1 December 2020	These requested documents have been transmitted on 17 & 18 March 2023: - R-ICD-AT-06.02.14-Map Agency Technical Instruction AI Tech 06.02.14 Service Interface Profile for Geospatial Services - Map Rendering Service 16 September 2016 - R-ICD-JOCWatch JOCWatch 4.1 Interface Control Document Oct 2022 - R-ICD-Namis Interface Control Document NAMIS v3.4.16 version 1.0 date 21/11/2018 - R-ICD-NCOP2 Interface Control Document NCOP2 ICD 7 June 2022 - R-ICD-TOPFAS-DM TOPFAS Increment-2 Software Design Specification Annex 1: Database Model (Desktop) 8/5/2020 - R-ICD-TOPFAS-ICD TOPFAS Increment-2 Software Design Specification Annex 3: Interface Control Document (Desktop) 15/09/2020 - R-ICD-TOPFAS-Excel Empty Plan Collecting Sheet Months All Collectors Dated December 2022 - R-ICD-LOGFAS LOGFAS INTERFACE CONTROL DOCUMENT 30-Jan-23 Version 8.0.0 The remaining documents requested will be transmitted, except for: Note that STANAG 4774 and 4778.2 (included in document delivery) instead of [R-ICD-IEGC] shall be used.
32		ASOP-07.01.25 (NCI Academy Standard Operating Procedure - Grading and Assessment, May 2020)	This document will be transmitted.
33		NATO-Bi-SC-DIR-075-007 (NATO Bi-SC Education and Individual Training Directive (E&ITD) 075-007, September 2015)	This document will be transmitted.
34		[AI-16.31.03] NCIA - Agency Instruction 16.31.03, Requirements for the preparation of IPSP, Sep 2022	This document will be transmitted.
35		SOAIDM-SDS-APPL_SERVICES	Under Consideration
36		SOAIDM-SDS-OBSERVABILITY	Under Consideration
37		SOAIDM-SDS-LIFECYCLE_AUTOMATION	Under Consideration
38		SOAIDM-SDS-INSTALLER	Under Consideration
39		SOAIDM-SDS-ANNEXES	Under Consideration
40		ITM-SDP	All ITM related requirements are generically provided in SRS and therefore are not provided separately as part of this IFB
41		R-ITM	All ITM related requirements are generically provided in SRS and therefore are not provided separately as part of this IFB
42		Ref-CPP-MJO+	Under Consideration
43		Ref-ATP-A2SL	Under Consideration
44		NU_CO-13703-ITM_2.2.2_SDP_IaaS_v1.8	This document is not directly referenced in IFB, therefore not considered relevant for bid preparation and therefore are not provided separately as part of this IFB
45		DEMETER ICD	Unclear what bidder is requesting, DEMETER is the new Land C2 system to be delivered, therefore no ICD yet exists
46		Information Exchange Requirements (IERs) [MC 593/1] Minimum Level of Command and Control (C2) Service Capabilities in Support of Combined Joint NATO Led Operations	This document will be transmitted.
47		Information Exchange Requirements (IERs) [MC 0640] NATO Minimum Scale of Communications and Information Systems (CIS) Capabilities in the Land Tactical Level	This document will be transmitted.
48		SOA IDM Latest Release with All Annexes (Wave 2)	Under Consideration
49		R-4774-CMLS	This document will be transmitted.
50		[NREF-11][AC/322-D(2019) 0038 (INV) CIS Security Technical and Implementation Directive for the Security of Web Applications.]	This document will be transmitted.
51		[R-4774-CMLS]	This document will be transmitted.
52		[R-4778.2-BindProf]	This document will be transmitted.
53		AGeoP-26 Ed A Ver 1 Defence Geospatial Web Services	Not directly referenced in IFB, therefore not considered relevant for bid preparation
54		AGeoP-08 Ed B Ver 1 NATO Geospatial Metadata Profile	Not directly referenced in IFB, therefore not considered relevant for bid preparation
55		AGeoP-11 Ed B Ver 1 NATO Geospatial Information Framework	Not directly referenced in IFB, therefore not considered relevant for bid preparation
56		STANAG 6523 Ed 1 Geospatial Web Services	Not directly referenced in IFB, therefore not considered relevant for bid preparation
57		STANAG 2586 Ed 2 NATO Geospatial Metadata Profile - AGeoP-8 Edition B	Not directly referenced in IFB, therefore not considered relevant for bid preparation
58		STANAG 2592 Ed 2 NATO Geospatial Information Framework - AGeoP-11(B) Ver. 1	Not directly referenced in IFB, therefore not considered relevant for bid preparation
59	04-IFB-CO-115791-DEMETER-Book I - Annex E - Eval Criteria to Reqt Matrix.pdf tab "Criteria To Requirements" line 106	E23.06 is not linked to SRS requirements. Is this intentional?	SRS requirements are guidance for evaluation criteria , if there is no associated requirement, evaluation criteria shall be considered as is.
60	SOW Annex A, Page 9 SRS-027	This requirement refers to [NREF_JOEL] which is not mentioned in Chapter 2 of the SRS nor in 04-IFB-CO-115791-DEMETER-Book I - Annex E - Eval Criteria to Reqt Matrix.xslx (References tab). Could you please provide the referenced document which should be included in the IFB document pack?	Use (NU) AC35-D(2002)-Directive on the Security of Information Rev 3

61	SOW Annex A, Page 10 SRS-029	This requirement refers to [NREF_TIDE] which is not mentioned in Chapter 2 of the SRS nor in 04-IFB-CO-115791-DEMETER-Book I - Annex E - Eval Criteria to Reqt Matrix.xslx (References tab). Could you please provide the referenced document which should be included in the IFB document pack?	Use (NU) AC35-D(2002)-Directive on the Security of Information Rev 3
62	SOW Annex A, Page 11 SRS-039	This requirement refers to [N-JOEL] which is not mentioned in Chapter 2 of the SRS nor in 04-IFB-CO-115791-DEMETER-Book I - Annex E - Eval Criteria to Reqt Matrix.xslx (References tab). Could you please confirm that the reference should be [NREF_JOEL] or else provide the referenced document which should be included in the IFB document pack?	Under Consideration
63	SOW Annex A, Page 15 SRS-063	This requirement refers to [REF_CCIR] which is not mentioned in Chapter 2 of the SRS nor in 04-IFB-CO-115791-DEMETER-Book I - Annex E - Eval Criteria to Reqt Matrix.xslx (References tab). Could you please provide the referenced document which should be included in the IFB document pack?	Under Consideration
64	SOW Annex A, Page 44 SRS-0248	This requirement refers to [R-ITM] which is not mentioned in Chapter 2 of the SRS nor in 04-IFB-CO-115791-DEMETER-Book I - Annex E - Eval Criteria to Reqt Matrix.xslx (References tab). Could you please confirm that the reference should be [R-ICD-SOA_IdM], or else provide the referenced document which should be included in the IFB document pack?	Under Consideration
65	SOW Annex A, Page 50 SRS-287	This requirement refers to [MC 593/1, MC 0640] which is not mentioned in Chapter 2 of the SRS nor in 04-IFB-CO-115791-DEMETER-Book I - Annex E - Eval Criteria to Reqt Matrix.xslx (References tab). Could you please provide the referenced document which should be included in the IFB document pack?	These documents will be transmitted.
66	SOW Annex A, Page 12 SRS-042	This requirement mentions “NATO formal message communication platforms (AIMS, NMS)”. Could you provide information on what these communication platforms are?	Under Consideration
67	SOW Annex A, Page 12 SRS-042	This requirement mentions “ORDERS in the correct format APP 11 (D)(1) so that it can be transferred to the destination with NATO formal message communication platforms (AIMS, NMS) manually”. Could you elicit what “manually” means in the context of this requirement?	Under Consideration
68	SOW Annex A, Page 44 SRS-250	This requirement mentions “NERS environment”. Can you provide information on this environment?	Under Consideration
69	SOW Annex A SRS-207	The verification method of this requirement is set to "Test". However it seems that this requirement can be best verified by inspecting the maintenance procedures. Would you consider changing the verification method to "Inspection"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
70	SOW Annex A SRS-279	The verification method of this requirement is set to "Test". However it seems that this requirement can be best verified by inspecting project documentation. Would you consider changing the verification method to "Inspection"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
71	SOW Annex A SRS-005	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
72	SOW Annex A SRS-007	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
73	SOW Annex A SRS-008	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
74	SOW Annex A SRS-080	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
75	SOW Annex A SRS-085	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
76	SOW Annex A SRS-086	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
77	SOW Annex A SRS-088	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
78	SOW Annex A SRS-089	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
79	SOW Annex A SRS-109	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
80	SOW Annex A SRS-110	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
81	SOW Annex A SRS-111	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
82	SOW Annex A SRS-144	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
83	SOW Annex A SRS-145	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.

84	SOW Annex A SRS-166	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
85	SOW Annex A SRS-168	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
86	SOW Annex A SRS-274	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
87	SOW Annex A SRS-275	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
88	SOW Annex A SRS-277	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
89	SOW Annex A SRS-280	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
90	SOW Annex A SRS-282	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
91	SOW Annex A SRS-283	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
92	SOW Annex A SRS-288	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
93	SOW Annex A SRS-289	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
94	SOW Annex A SRS-307	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
95	SOW Annex A SRS-308	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
96	SOW Annex A SRS-309	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
97	SOW Annex A SRS-311	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
98	SOW Annex A SRS-312	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
99	SOW Annex A SRS-320	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
100	SOW Annex A: SRS-328	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
101	SOW Annex A: SRS-330	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
102	SOW Annex A: SRS-331	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
103	SOW Annex A: SRS-332	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
104	SOW Annex A: SRS-333	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
105	SOW Annex A SRS-334	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.

106	SOW Annex A SRS-335	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
107	SOW Annex A SRS-336	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
108	SOW Annex A SRS-344	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
109	SOW Annex A SRS-347	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
110	SOW Annex A SRS-348	The verification method of this requirement is set to "Test". However, it seems that verifying it is possible without "instrumentation, other special test equipment or specific test patterns to collect data for later analysis" (from section 1.4.3). Would you consider changing the verification method to "Demonstration"?	• These are suggested verification methods. • Refer to SOW paragraphs 4.2.1 and 8.13 which describe how this will be managed during the contract.
111	SOW Annex A Chapter 2 pages 3 and 4	This Chapter refers to "AD 80-84 NATO Recognized Ground Picture". Could you please provide this document which should be included in the IFB document pack?	This document will be transmitted.
112	SOW Annex A Chapter 2 pages 3 and 4	This Chapter refers to "NATO Policy on Cyber Defence". Could you please provide this document which should be included in the IFB document pack?	This document has been transmitted on 17 / 18 March 2023.
113	SOW Annex A Chapter 2 pages 3 and 4	This Chapter refers to "Command and Control of Allied Land Forces". Could you please provide this document which should be included in the IFB document pack?	This document has been transmitted on 17 / 18 March 2023.
114	SOW Annex A Chapter 2 pages 3 and 4	This Chapter refers to "NATO Communications and Information Agency Costed Customer Services Catalogue v7.1 2023Service Definitions". Could you please provide this document which should be included in the IFB document pack?	This document has been transmitted on 17 / 18 March 2023.
115	SOW Annex A Chapter 2 pages 3 and 4	This Chapter refers to "PO(2021)0360 Data Exploitation Framework Policy". Could you please provide this document which should be included in the IFB document pack?	This document will be transmitted.
116	SOW Annex A Chapter 2 pages 3 and 4	This Chapter refers to "To be delivered". Could you please provide this document which should be included in the IFB document pack?	Under Consideration
117	Book I - Annex E - Eval Criteria to Reqt Matrix	There are no System Requirements Specifications for the Engineering Criteria E19, which relates to Training. Is this intentional?	Under Consideration
118		[AC322-D(2019)0034 (INV)] C3B -Consultation Command & Control Board C3 TAXONOMY BASELINE 3.1	This document will be transmitted.
119		[ACMP-2009-SRD-41] Examples of Configuration Management Plan Requirements, Ed.A V1, Mar 2017	This document will be transmitted.
120		[ACMP-2100] The Core Set of Configuration Management Contractual Requirements, Ed.A V.2, Mar 2017	This document will be transmitted.
121		[AD-070-001] ACO Directive 070-001 Allied Command Operations Security Directive, Dec 2021	This document will be transmitted.
122		[AI-16.31.03] NCIA - Agency Instruction 16.31.03, Requirements for the preparation of IPSP, Sep 2022	This document will be transmitted.
123		[ALP-10] NATO Guidance on Integrated Logistics Support for Multinational Armament Programs, Ed.C V1, 2017	This document will be transmitted.
124		[AQAP 4107] Mutual Acceptance of Government Quality Assurance and Usage of the Allied Quality Assurance Publications, Edition A, Version 2, Nov 2018	This document will be transmitted.
125		[AQAP-2070] NATO Mutual Government Quality Assurance (GQA) Process	This document will be transmitted.
126		[AQAP-2105] NATO Requirements for Quality Plans, Ed.C V1, Jan 2019	This document will be transmitted.
127		[AQAP-2110] NATO Quality Assurance Requirements for Design, Development and Production, Ed.D V1, Jun 2016	This document will be transmitted.
128		[AQAP-2210] NATO Supplementary SQA Requirements to AQAP-2110 or AQAP2310, Ed.A V2, Sep 2015	This document will be transmitted.
129		[ASD-AIA-SX000i] International Specification for Integrated Product Support (IPS), Issue No.3.0, Apr 2021	This document is available on the internet: https://www.sx000i.org/docs/SX000i%20Issue%203.0.pdf
130		[ASD-S3000L] International Procedure Specification for Logistic Support Analysis (LSA), Issue No.2.0, Apr 2021	This document is available on the internet: https://www.s3000l.org/docs/S3000L%20Issue%202.0.pdf
131		[ASOP-07.01.25] NCI Academy Standard Operating Procedure - Grading and Assessment, May 2020	This document will be transmitted.
132		[C-M(2002)49] Security within the North Atlantic Treaty Organization	This document will be transmitted.
133		[C-M(2015)0041] Alliance C3 Policy	This document will be transmitted.
134		[ISO/IEC/IEEE-29119] International Standard for Software Testing, 2022	This document is available on the internet: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
135		[ISO/IEC/IEEE-29148] International Standard for Systems and software engineering – Life cycle processes – Requirements engineering, 2011	This document can be obtained from ISO, see: https://www.iso.org/standard/72089.html
136		[ISO-9000:2015] Quality management systems – Fundamentals and vocabulary	This document can be obtained from ISO, see https://www.iso.org/standard/45481.html
137		[NATO-Bi-SC-DIR-075-007] NATO Bi-SC Education and Individual Training Directive (E&ITD) 075-007, Sep 2015	This document will be transmitted.
138		[NCIA-AD-06.00.16] NCIA - Agency Directive 06.00.16, Configuration Management, Feb 2020	This document will be transmitted.
139		[NCIA-AI-23.02] NCIA - Agency Instruction 23.02, Deployment Management Planning, Oct 2019	This document will be transmitted.
140		[NCIA-AI-TECH-06.03.01] NCIA - Agency Instruction 06.03.01, Identification of Software Assets, Jun 2016	This document will be transmitted.
141		[NCIA-SOP-06.03.05] NCIA – Agency Standard Operating Procedure 06.03.05, Software Patch Management, Oct 2020	This document will be transmitted.
142		[NCIA-SOP-23.01] NCIA – Agency Standard Operating Procedure 23.01, Enterprise IT Change Management, Mar 2020	This document will be transmitted.
143		[NREF-JOEL] Not in reference lists, but referenced from SRS-017 etc.	This document will be transmitted.
144		[Ref-ATP-A2SL] Not in reference lists, but referenced from SRS-296	Under Consideration
145		[Ref-DEFP] PO(2021)0360 Data Exploitation Framework Policy	This document will be transmitted.

146		[R-ICD-FasInterop] TOPFAS/LOGFAS ADL-FPH ORBAT Schemas version 2022.7	This document will be transmitted.
147		[R-ICD-IEGC]	Use STANAG 4774 and 4778.2 (included in document delivery) instead.
148		[R-ICD-Intel-FS-DM] CO-115718-I2BE, INTEL-FS Spiral 2 NAF 4.0 L7 Information Model Data Dictionary - All Entities Nov 8, 2022 4:58 PM	This document will be transmitted.
149		[R-ICD-NIRIS] Track Store Open API interface – original version to be provided	This document will be provided as soon as possible.
150		[R-ICD-SOA_IdM] CO-14176-SOA-IDM Service Oriented Architecture (SOA) and Identity Management Platform (IdM) Wave I Interface Control Document (ICD) Doc. Version: 15.0 Date: 08/06/2021	Under Consideration
151		[R-ITM] Not in reference lists, but referenced from SRS-248	R_ITM shall be ignored, the specifications of any system that shall operate in NATO enterprise environments are stated in SRS.
152		[R-RGP] AD 80-84 NATO Recognized Ground Picture	This document will be transmitted.
153		[R-SharePoint] Standard SharePoint message and content exchange protocols	Under Consideration
154		[SOA-IdM] SOA-IDM Service Oriented Architecture (SOA) and Identity Management (IdM) Platform - Wave 1 - Interface Control Document (ICD) V15.0, Jun 2021 - System Design Specification (SDS) V9.3, May 2021	Under Consideration
155		[STANAG-4107] Mutual Acceptance of Government Quality Assurance and Usage of the Allied Quality Assurance Publications	This document will be transmitted.
156		[STANAG-4427] Edition 3 - Configuration Management in System Life Cycle Management	This document will be transmitted.
157		[XSD-LC2IS] Interface Control Document (ICD) for LC2IS Inc 2 Contract no CO14463-LC2IS F0057 62794795 558 Rev M - Annex E LC2IS Inc 2 XML Schema Definition	Under Consideration
158		Why is the price limit divided into CLINs 1-3 and 4, if CLINs 1-2 are basic and CLINs 3-4 are optional? Whether the price limit should refer to CLIN 1-2 and 3-4?	Under Consideration
159		In the labor tab there is only one column to enter labor rate (column „O"). Is it allowed to add columns to enter Unit Cost per MD for subsequent years?	Under Consideration
160	02-IFB-CO-115791-DEMETER-AMD1 Book I-Annex A-Bidding Sheets Tab "CLIN Summary"	Could you please precise in which CLIN do we include the WP3 initiation phase? The bidding sheet doesn't mention the §4.2.x as done in CLINs 1.2.1/1.2.2/2.2.1/2.2.2.	Under Consideration
161	02-IFB-CO-115791-DEMETER-AMD1 Book I-Annex A-Bidding Sheets Tab "CLIN Summary"	Could you please confirm that we have to include the Project Management costs in the M&S CLINs?	Under Consideration
162	02-IFB-CO-115791-DEMETER-AMD1 Book I-Annex A-Bidding Sheets Tab "CLIN Summary"	Due to the COTS support model, the licensing policy supports M&S costs. Can we indicate license cost only for that part?	Under Consideration
163	02-IFB-CO-115791-DEMETER-AMD1 Book I-Annex A-Bidding Sheets Tabs "Labour, Material, Travel"	We understand that the contract will last for 12 years & two months. However the bidding sheets file only presents columns for ten years to indicate man days (idem for Material & Travel) per year. Could you please confirm there is no mistake? If not, how do we proceed for CLINs 4.8/4.9/4.10	Under Consideration
164	02-IFB-CO-115791-DEMETER-AMD1 Book I-Annex A-Bidding Sheets & 01-IFB-CO-115791-DEMETER-AMD1 Book I-Bidding Instructions	Given the fact that there is an economic price adjustment formula, the bidding sheets only takes into account current (2023) labour cost and others (tab Rates). Could you please confirm that the bidding sheets file must only be based on current costs when the price evaluation takes into account a calculated present value?	Under Consideration
165	02-IFB-CO-115791-DEMETER-AMD1 Book I-Annex A-Bidding Sheets Tab "Payment Schedule" & 08_IFB_CO-115791-DEMETER-Book-II-Part-IV-Statement of Work (SOW),§1.4	The SOW and the bidding sheets file indicate different dates for the PSA & FSA WP2 milestones for the project. Could you please indicate which one is correct? (Payment Schedule tab & SOW §1.4)	Under Consideration
166		To be able to provide our best offer, we kindly request an extension of the Bid Closing Date of at least 1 month.	Under Consideration
167		Could you please confirm if we can sign the documents electronically with an Official Certificate or if it must be a handwritten signature?	Under Consideration
168	BOOK II, Part II Contract Special Provisions, 17.9 BOOK II, Part III Contract General Provisions, 30.2.2	If we deliver COTS software (within the scope of WP1 and WP2) the provisions of Sec. 17.9 of BOOK II, Part II Contract Special Provisions and sec. 30.2.2 of BOOK II, Part III Contract General Provisions saying about unlimited number of users (or licenses) do not apply (i.e. COTS are purchased in a specific number of licenses)? However, in case when we modify the COTS software by adding new functionalities within the scope of WP3, then such COTS software, which is the base for derivative product (final product), is to be understood as Contractor Background IPR and according to above provisions can be used and exploit by an unlimited number of users within NATO and NATO members?	Under Consideration
169	06_IFB-CO-115791-DEMETER_Book II-Part II Special Provisions, Article 14	The confidentiality and non-disclosure provisions set out in Article 14 of Part II Contract Special Provisions are currently drafted as one-way. A variation is requested to ensure that the confidentiality and non-disclosure provisions are reciprocal in the final drafting.	Under Consideration

170	07-IFB-CO-115791-DEMETER-Book II-Part III-Contract General Provisions, Clause 14.2	This clause provides that the Facility Representative will determine whether the Purchaser's Facilities are provided free of charge, or determine what charges are payable. For transparency and understanding, please can you provide clarity as to the assessment criteria for determining when the charges will apply i.e. only in the event of re-test, and the relevant price list?	Under Consideration
171	07-IFB-CO-115791-DEMETER-Book II-Part III-Contract General Provisions, Clause 16	This clause provides a unilateral change control process requiring the Contractor to act as if a change control has been approved until advised otherwise, irrespective of whether the Contractor agrees or considers the work achievable etc. Requiring the Contractor to proceed with the change as part of the contract prior agreement (as per clause 16.7) is an unusual and onerous clause which could lead to avoidable dispute or breach. A variation is requested, amending the change control process to a mutual process, requiring the agreement of both the Contractor and Purchaser prior to a change forming part of the binding contract scope.	Under Consideration
172	07-IFB-CO-115791-DEMETER-Book II-Part III-Contract General Provisions, Clause 19.3 and 07-IFB-CO-115791-DEMETER-Book II-Part III-Contract General Provisions, Clause 28	These clauses provide for a full right of audit, including an audit of pricing. A waiver is requested so that any such audit relates only to bespoke development and other services provided under the contract, but does not permit inspection and interrogation of prices, development processes and other data as it relates to third party COTS products.	Under Consideration
173	06_IFB-CO-115791-DEMETER_Book II-Part II Special Provisions, Article 6.7 Part II And 07-IFB-CO-115791-DEMETER-Book II-Part III-Contract General Provisions, Clause 25.7	Please can the Purchaser confirm that Article 6.7 Part II Contract Special Provisions replaces clause 25.7 General Contract Provisions rather than supplementing it?	Under Consideration
174	07-IFB-CO-115791- DEMETER-Book II-Part III-Contract General Provisions, Clause 21.7	Purchaser remedies available under this contract provide that the Purchaser can elect, at their sole discretion, to have the contractor fix defects, require all information to be passed to Purchaser to allow Purchaser to remedy any defect with Contractor covering the costs, or for there to be a reduction in contract value. A variation is requested to define an order of precedence in respect of these remedies, and to enable the Contractor an opportunity to take remedial action in the first instance. Only where the Contractor fails to remedy within a reasonably agreed timeframe, or where there is termination following breach, shall the Purchaser seek to remedy the defect itself or through third parties, with any additional costs being charged to the Contractor.	Under Consideration
175	06_IFB-CO-115791-DEMETER_Book II-Part II Special Provisions, Article 22 Part II	This Article, in its current drafting, is contrary to standard software maintenance provisions which provide for bug fixes, new releases etc. to be made available as part of the maintenance package. A waiver is therefore requested for this Article. Alternatively, if the intent of this Article was to address instances where a COTS product is discontinued and a new product is released in its place (distinct from upgrades etc. as part of maintenance), a variation is requested to remove the language referring to upgrades in order to add clarity to this Article.	Under Consideration
176	07-IFB-CO-115791- DEMETER-Book II-Part III-Contract General Provisions, Clause 42.6	A waiver is requested of clause 42.6 as it unreasonably restricts the legal recourse of the Contractor in the event of dispute. Whilst it is the intention of the parties in the event of any dispute to follow the dispute resolution procedures and seek to reach settlement by mutual agreement, and further to furnish the Contracting Authority with all facts, evidence and proof during the early dispute resolution process, the Contractor cannot be limited in arbitration only to that evidence previously identified and issued previously raised, as other matters may become evident throughout the process. It is agreed that reasonable efforts should be taken to ensure that all matters are raised, and facts, evidence and proof produced to the Contracting Authority in advance, but to limit disclosures and remedies as per the current drafting is inequitable.	Under Consideration
177	07-IFB-CO-115791- DEMETER-Book II-Part III-Contract General Provisions, Clause 42	It is usual in arbitration clauses to define the language of arbitration, but this is not specified in clause 42 General Contract Provisions. A variation is requested to specify the language of arbitration as English in the final drafting.	Under Consideration
178	07-IFB-CO-115791- DEMETER-Book II-Part III-Contract General Provisions, Clause 31.6	The COTS product does not include all required information detailed at clause 31.6 as standard. To include this would result in development of a bespoke release of the COTS product specific to NATO meaning that it would not be part of the standard COTS roadmap. As such a variation to clause 31.6 is requested to exclude COTS products. It is proposed that this information instead be provided in a cover sheet or separate read- me file.	Under Consideration
179	01-IFB-CO- 115791-DEMETER-Book I-Bidding Instructions, Clause 4.8, Post Evaluation Test Drive	The bidder understands that a post evaluation test drive will be conducted with the winner selected from the best value exercise. In order to get the best value out of this tender process, the bidder recommends the following changes to the post evaluation test drive: 1. The test drive should be conducted with the the three highest scored bidders from the best value exercise. 2. 4.8.1.4 should be changed to that all evaluation criteria in TVCRM that is marked as COTS available should be tested. 3. 4.8.3.3.6 should be changed so an unsuccessful test drive will determine the Bidder's Offer to be non-compliant.	Under Consideration

180	Book II Part III-Contract General Provisions §21, page N°25 21.8	*"When NQAR is not applicable based on the scale of the project, the Purchaser reserves the right to perform inspections through his own staff in accordance with the latest ISO standard at the time of inspection."* *Could you confirm that Contractor shall comply with the latest ISO standard at the time of contract signature? Could you confirm that it is also valid for other standards (administrative or technical)?*	Under Consideration
181	Book II Part II – Contract Special provisions – § 17, page N°17, 17.5	*"This licence shall also allow the Purchaser and its member nations to use and authorise others to use the software for further adaptation, integration, modifications and future procurements."* *Could you confirm that this article applies to the Foreground IPR only?* *Could you define "others"?*	Under Consideration
182	Book II Part II – Contract Special provisions – § 17, page N°17, 17.7	*"The Contractor warrants, undertakes, and represents that any derivative product created under this Contract from the stated Background IPR shall be considered as Foreground IPR and, therefore, shall be governed by the terms and conditions specified in Clause 30.3 (Foreground IPR) of the Contract General Provisions."* *Could you confirm that a derivative product is restricted to the adaptations realized in WP3? If not, could you define a derivative product?*	Under Consideration
183	08_IFB_CO-115791-DEMETER-Book-II-Part-IV-Statement of Work (SOW), [SOW-526]	What is the impact of having AQAP certificates of approval (2110, 2210 or 2310) on the requirement related to approval of QA procedures aspects?	Under Consideration
184	07-IFB-CO-115791-DEMETER-Book II-Part III-Contract General Provisions,§30.2.2 & 06_IFB-CO-115791-DEMETER_Book II-Part II Special Provisions,§17.8 & 02-IFB-CO-115791-DEMETER-AMD1 Book I-Annex A-Bidding Sheets & 08_IFB_CO-115791-DEMETER-Book-II-Part-IV-Statement of Work (SOW),§3.6, [SOW-038]	The Special provisions and the SOW ask for no additional fee due to further re-transfer of the software or additional end user while the bidding sheet asks for a price to cover a right to use for 500 users. Considering a lot of COTS have a license model based on numbers of users, instances, capacities, would you mind to align the different related clauses in the Special provisions and SOW to take into account these existing licensing models and the limit fixed of 500 users?	Under Consideration
185	01-IFB-CO-115791-DEMETER-Book I-Bidding Instructions.pdf	Can you confirm that a criterion (or top-level criterion) is a line in the TVCRM with value 3 in column B of the TCVRM?	Under Consideration
186	01-IFB-CO-115791-DEMETER-Book I-Bidding Instructions.pdf	Can you confirm that a sub criterion is a line in the TVCRM with value 4 in column B of the TCVRM?	Under Consideration
187	01-IFB-CO-115791-DEMETER-Book I-Bidding Instructions.pdf § 4.2.5.3 page 26	"The sub criteria are listed in descending order which reflects the relative importance that the Purchaser places on each sub criterion". Is the descending order relative to the whole set of sub criteria (value 4 in column B of the TCVRM) or does the descending order reflect Purchaser's priorities within each top-level criterion (value 3 in column B of the TCVRM)?	Under Consideration
188	01-IFB-CO-115791-DEMETER-Book I-Bidding Instructions.pdf § 3.5.5.2. page 21	Can the mapping of a sub-criterion include several sections of the Technical Bid?	Under Consideration
189	01-IFB-CO-115791-DEMETER-Book I-Bidding Instructions.pdf § 4.8.1.5	"The Test Drive will be deemed successful if all Test Scenarios in the Final Test Plan are successfully demonstrated per the Acceptance criteria defined by the Purchaser": when will the Acceptance criteria be made available to the apparent winner?	Under Consideration
190	01-IFB-CO-115791-DEMETER-Book I-Bidding Instructions.pdf § 4.5.2.1.2	"For each of the listed engineering criteria and sub-criteria". Can you confirm that this should read "For each of the listed engineering sub-criterion"?	Under Consideration
191	01-IFB-CO-115791-DEMETER-Book I-Bidding Instructions.pdf § 4.3.3.3.2.	This para refers to "a composite score […] in any of the sub-criteria". What does the term "composite score" refer to?	Under Consideration

192	01-IFB-CO-115791-DEMETER-Book I-Bidding Instructions.pdf § 4.3.3.3.2.	This para refers to "a composite score of less than 20% of the maximum score possible in any of the sub-criteria". What method will be used to compute both the maximum score and the composite score of a bidder at sub-criterion level?	Under Consideration
193	01-IFB-CO-115791-DEMETER-Book I-Bidding Instructions.pdf § 3.2.1.	The filename required for technical videos is "115791-DEMETER-Company Name–Vol-III– Tech005-Part I-Technical-Videos-NoX.mp4 (where 'X' is number)". Since Powerpoint files are acceptable, can we assume that their filename would be "115791-DEMETER-Company Name–Vol-III– Tech005-Part I-Technical-Videos-NoX.ppt (where 'X' is number)"?	Under Consideration
194	01-IFB-CO-115791-DEMETER-AMD1 Book I-Bidding Instructions	Could you please confirm that the post evaluation test drive won't address features that are planned as part of the product roadmap (sub-criterion S02.01)?	Under Consideration
195	01-IFB-CO-115791-DEMETER-AMD1 Book I-Bidding Instructions	How will the product roadmap (features under development that will be available for WP2) be considered in the bid's engineering notation?	Under Consideration

STANDARDS RELATED DOCUMENT

ACMP-2009-SRD-41

EXAMPLES OF CM PLAN REQUIREMENTS

Edition A Version 1
MARCH 2017

NORTH ATLANTIC TREATY ORGANIZATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

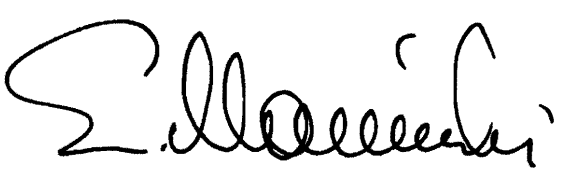
NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

6 March 2017

1. The enclosed Standards Related Document, ACMP-2009-SRD-41, Edition A Version 1, EXAMPLES OF CM PLAN REQUIREMENTS, which has been approved in conjunction with ACMP-2009, by the nations in the AC/327 Life Cycle Management Group, is promulgated herewith.

3. This publication shall be handled in accordance with C-M(2002)60.



Edvardas MAŽEIKIS
Major General, LTUAF
Director, NATO Standardization Office

INTENTIONALLY BLANK

EXAMPLES OF DELIVERABLE CM PLAN REQUIREMENTS

Purpose:

The purpose of this publication is to offer the Acquirer some options, examples of control over the format and content of Supplier CM Plans. Such controls should be used in conjunction with the NATO Clause below, and are recommended only for supplier CMPs which need Acquirer approval and are deliverables in the contract.

NATO Clause:

4.3	The format of the CMP shall conform to the outline and format specified in REFERENCE. Optionally, sections listed may be further subdivided.

REFERENCE # 4.3.A - Reference ISO 10007:2003(E)

*"ISO 10007:2003, Annex A , Structure and content of a configuration management plan, is **mandatory** for this contract.*

REFERENCE # 4.3.B - Reference EIA-649-1

The Supplier's CMP shall comply with the requirements of DI-SESS-80858, Supplier's Configuration Management Plan

---

REFERENCE # 4.3.C (Derived from ACMP-1 Ed2)

*The Supplier's CMP shall comply with the requirements ..***see below**

REFERENCE # 4.3.D - Derived from MIL-STD-973)

The Supplier's CMP shall comply with the requirements.. **see below**

REFERENCE # 4.3.E – Reference ASD-STAN prEN 9223-100:2016

*"ASD-STAN prEN 9223-100:2016, Annex B, Structure and content of a configuration management plan, is **mandatory** for this contract.*

REFERENCE # 4.3.C (Derived from ACMP-1 Ed2)

The Supplier's CMP shall comply with the requirements below:

1. General

1.1 The Configuration Management Plan (CMP) shall define the organization and procedures used for the configuration management of the functional and physical characteristics of CI, including interfaces and configuration identification documentation. Unless otherwise specified in the contract, the CMP shall be prepared in accordance with the requirements contained herein. The language of the CMP shall be as described in the contract.

1.2 Objectives

1.2.1 In preparing the CMP the supplier shall:

a. ensure that all required elements of CM are applied in such a manner as to provide a comprehensive CM program;
b. identify the means by which continuity of effort and understanding is achieved between his sub-suppliers and himself, and between the PM and himself and internally within his organization, for the allocated CI, integrating, interfacing or otherwise related CI, supplier organizations, test and evaluation activities, and managers; and
c. establish his internal CM requirements for the contract.

1.3 Implementation

1.3.1 Unless otherwise stated in the contract, the CMP shall be delivered to the PM for approval, no later than thirty (30) days, after contract award. Depending on contract duration, updating of the CMP may be necessary. Procedures and the schedule for such updating shall be provided by the supplier or included in the CMP itself. The CMP, when approved, shall serve as a working document to plan, guide, and measure the CM process. CM shall be implemented in accordance with the approved CMP.

2. Detailed Requirements

2.1 CMP Format

The format of the CMP shall conform to the following outline. Optionally, sections listed may be further subdivided.

a. Cover Page
b. Record of Reviews and History
c. Contents Page
d. Introduction
    (1) Purpose and Scope
    (2) Description of the CI
    (3) Definitions

(4) Project Phasing and Milestones
(5) Special Features

e. Organization
(1) Project Management Structure
(2) Configuration Management Structure
(3) Configuration Management Personnel
(4) Configuration Control Board
(5) Policy Directives
(6) Reference Documents
(7) Sub-supplier / Vendor Control

f. CM Responsibilities Configuration Identification and Documentation
(1) Selection and Description of the CI
(2) Identification of the CI
(a) Hardware CI Identification
• Part/Item Numbering
• NATO Supply Code for Manufactures
• Additional Numbering
• Serial/LOT Numbering
(b) Computer Software CI Identification
• Computer Program Identification
• Software File Identification
• Source File Identification
• Executable File Identification
• Patch Identification
• Build Identification
• Firmware Identification
(3) Nomenclature
(4) Product Marking and labelling.
(5) Configuration Documentation
(a) Document Numbering
(6) Configuration Baselines
(a) Functional Baseline (FBL)
(b) Allocated (development) Baseline (ABL)
(c) Product Baseline (PBL)
(7) Documentation library.
(8) Drawing library.
(9) Software Development Library.
(10) Engineering Release System
(a) Engineering Release Record

g. Configuration Control
(1) Configuration Control Board
(2) Configuration Changes Procedures
(a) Processing of Engineering change proposals.
(b) Notice of Revision.
(c) Request for Deviations and Waivers.
(3) Parts Substitution.

(4) Interface Management
(a) Documentation
(b) Interface Control
(c) Interface Control Working Group (ICWG)

h. Configuration Status Accounting and Configuration Data Management.
(1) Configuration Data Handling.
(2) Reporting.
(3) Configuration Data access
(4) Configuration Management Metrics.

i. Configuration Audits

j. Technical Reviews

2.2 CMP Content

The information described in the following paragraphs shall be included in each supplier CMP, as applicable.

Cover Page. The cover page shall provide the name and CI number of the top level CI to which this CMP applies, the supplier's name and address, contract umber,
Contract Data Requirements List sequence number, the PM name and address, and date of issue. This page shall also contain the suppliers authorizing signature and an approval / signature block for the PM.

Record of Reviews and History. This information shall include the history of approved changes to the plan, the approved dates of the changes and a small note describing each change.

Contents Page. Self-explanatory.

Introduction. The introduction shall contain the following paragraphs:

a. **Paragraph 1.1 - Purpose and Scope**. This paragraph shall state the purpose of the CMP and shall identify the materiel to which the plan is to be applied and the management/acquisition philosophy to which it is tailored.

b. **Paragraph 1.2 - Description of the CI.** The CI, or family of CI, shall be briefly described in this paragraph. Information will be provided in a manner to avoid security classification of the plan, if possible. Sufficient detail shall be presented to permit a basic understanding of the CI and its complexity. Included shall be the following:

(1) A description of the selection criteria and the associated rationale employed to select the CI;

(2) A description of key lower level CI (hardware and software) including training devices and simulators showing their relationship to the work breakdown structure of the complete project;

(3) A description of the function of the top level CI and its interrelationship to other system functions; and

(4) Government Furnished Equipment/Property. (May be specified in a separate appendix, if necessary).

c. **Paragraph 1.3 - Definitions**. This paragraph shall reference applicable directives or glossaries containing accepted definitions of terminology.

d. **Paragraph 1.4 - Project Phasing and Milestones**. The current status of the project shall be specified at the time of preparation or update of a CMP. A milestone chart shall be included which depicts the CM activities and their relationship to the major overall project milestones. The relationship between events critical to CM and to the schedule / control of the project shall be specifically defined. This should include the sequencing of design reviews, the release of engineering documentation, and the start of production, the test program, logistic support and audit events.

e. **Paragraph 1.5 - Special Features**. Special features of the materiel or the management program, which have a bearing on the application of CM, will be described here (e.g., major product improvement programs which will result in more than one configuration to be supported in the field with more than one product baseline, or major model differences in systems or weapons designed for varying applications). Peculiarities of the CM program that result from participation by a large number of organizations, or unique contracting methods (e.g., preproduction evaluation, use of many commercial items, use of existing drawings and specifications, or employment of an integrating supplier) will be described here. Innovations intended to increase the effectiveness of the CM program will also be described here.

Organization. This section of the CMP shall outline the relationship and integration of the supplier's project management and CM organizations and describe the organizational relationship of the individuals and activities involved in the CM program. The responsibilities of each individual or group shall be defined as well as the policy directives that govern the suppliers CM program.

a. **Paragraph 2.1 - Project Management Structure**. The supplier shall include an organization chart, which illustrates his project management structure. The chart, supplemented by a description or flow diagrams, shall illustrate the authority/responsibility of the key organizational elements impacted by contractual requirements for CM.

(1) **Paragraph 2.1.1 - Configuration Management Structure**. Charts supplemented by narrative descriptions shall define the relationships between activities directly involved in the CM program. The charts shall include the Configuration Manager, CM Office or function, interfacing organizations, procuring and administrative contracting officers, data management, and subsuppliers to the extent employed in the CM program and any other elements that may be involved. The integration of CM activities with other project activities shall also be described. This paragraph shall also identify the interrelationships, if applicable, among the supplier's software and hardware CM organizations. Each activity or individual shown on the organization chart(s) shall be the subject of a subparagraph, which will detail the authority and responsibility for which CM is assigned.

Signature authority for Engineering Change Proposals (ECP), Requests for Deviations (RFD) and Requests for Waivers (RFW) shall be specifically assigned.

(2) **Paragraph 2.1.2 - Configuration Management Personnel**. This paragraph shall describe by title and qualifications the positions which shall perform supplier CM.

(3) **Paragraph 2.1.3 - Configuration Control Board (CCB)**. This paragraph shall describe the organisational structure of the supplier's CCB. The following shall be included:

(a) Interrelationship of CCB if there is more than one level or separate software CCB;

(b) Membership of the CCB by organization and functional group; and

(c) Effective date of operational status (the CCB shall be in operational status when the functional baseline is established).

b. **Paragraph 2.2 - Policy Directives**. All policy directives (Government and supplier) directly related to CM shall be listed. These directives shall be project related directives or, if supplier standards, directly traceable to a project directive. If supplier standards are to be tailored for the project application, this shall be clearly defined in a cover project directive.

c. **Paragraph 2.3 - Reference Documents**. This paragraph shall list only those documents which are referred to in the CMP, with the exception of those listed in Paragraph 2.2.

d. **Paragraph 2.4 – Subsupplier / Vendor Control**. The supplier shall indicate his proposed methods for control over subsuppliers and vendors, insofar as it impacts on his CM commitments to the PM. The methods used to determine their capability and to monitor their ability to support the requirements of CM shall be explained.

e. **Paragraph 2.5 - CM Responsibilities**. The responsibilities of each individual or group shall be defined as well as the policy directives that govern the suppliers CM program. Charts supplemented by narrative descriptions shall define the relationships between activities directly involved in the CM program. The charts shall include the Configuration Manager, CM Office or function, interfacing organizations, procuring and administrative contracting officers, data management, and subsuppliers to the extent employed in the CM program and any other elements that may be involved. The integration of CM activities with other project activities shall also be described and interrelationships, if applicable, among the supplier's software and hardware CM organizations. Each activity or individual shown on the organization chart(s) shall be the subject of a sub-paragraph which will detail the authority and responsibility for which CM is assigned. Signature authority for Engineering Change Proposals (ECP), Requests for Deviation (RFD/W) shall be specifically assigned.

Configuration Identification and Documentation. This section shall describe the methods to be used for identifying (e.g., naming, marking, numbering) documents and physical items (CI) in accordance with ACMP-2. Methods to achieve configuration traceability from requirements to equipment, components, computer software, facility sites and spares shall also be described. Requirements for the preparation, submission and subsequent release of PM approved documentation which defines each of the required baselines shall also be described in this section. The supplier's methods under which the documentation will be prepared and released internally shall also be described.

a. **Paragraph 3.1 - Selection and Description of the CI**. The supplier shall select, recommend and obtain the approval of the customer for potential CI. The CI, or family of CI, shall be briefly described in this paragraph. Information will be provided in a manner to avoid security classification of the plan, if possible. Sufficient detail shall be presented to permit a basic understanding of the CI and their complexities.

b. **Paragraph 3.2 - Identification of the CI**. The supplier shall issue unique identifiers for the CI and the configuration documentation and maintain the configuration identification to facilitate effective logistics support of items in service.

(1) **Paragraph 3.2.1 - Hardware Configuration Item (HWCI) Identification**. The supplier shall identify his plans and procedures for HWCI and part identification, serialisation, and lot number, including the criteria to be used for part re-identification. This paragraph shall list the criteria used in applying serial numbers and lot numbers and shall identify, where possible by document number, the items that shall be subjected to serial / lot control. As well, this paragraph shall present the supplier's plans and identify his procedures and capabilities of generating and maintaining a record which describes the relationship between the "as designed," "as built," and "as modified" configurations.

(2) **Paragraph 3.2.2 - Computer Software Configuration Item (CSCI) Identification**. This paragraph shall describe the supplier's plans, procedures, and methods for identifying:

(a) Each CSCI;

(b) The version, release, change status, and any other identification details of each deliverable item;

(c) The version of each CSCI to which the corresponding software documentation applies;

(d) The software documentation and the computer software media containing code, software documentation or both that are placed under configuration control; and

(e) The specific version of software contained on a deliverable medium, including all changes incorporated since its last release.

c. **Paragraph 3.3 - Nomenclature**. This paragraph shall address the process of nomenclature assignment and the requirements for titling specifications and drawings.

d. **Paragraph 3.9 Product Marking and Labelling**. The supplier shall describe his method of marking and labelling CI (HW, SW, FW, NDI, COTS and PDI) and seek approval by the customer.

e. **Paragraph 3.4 - Documentation Numbering**. If the PM has specified requirements (assignment of numbers) for documents, those requirements shall be stated here. If supplier numbers are to be used, this paragraph shall describe the numbering system to be used for drawings and specifications.

f. **Paragraph 3.5 - Configuration Baselines**. The supplier shall list the documents with their format, review and release procedures and the degree of PM control which establish the Functional, Allocated and Product baselines shall be listed and addressed.

(1) **Paragraph 3.5.1 - Functional Baseline**. The documents, which establish the functional baseline, shall be listed in this paragraph. If the Functional Baseline is to be prepared by the supplier, the format of the document(s) will be specified by the PM. The procedure for review and release shall be outlined, and the degree of control by the PM shall be specified. The supplier's plan for proposing changes to those documents shall be described.

(2) **Paragraph 3.5.2 – Allocated Baseline**. A list of all existing and required specifications shall be included in specification tree format. A list of drawings, if applicable, which form a part of the Allocated Baseline shall also be provided. If the supplier is to prepare the documents for the Allocated Baseline, plans for preparation, review and release of the allocated documentation shall be outlined here. The supplier's plan for proposing changes to this baseline shall be outlined.

(a) **Paragraph 3.5.2.1 - Specifications**. This paragraph shall identify existing specifications or specifications that the supplier shall prepare for the CI or family of CI (by title, document number, issuing authority and date of issue), and the use of these specifications to establish and control the Allocated (development) Baseline. Any limitations on PM approval of specification format and content and at what stage in the project that specifications will be available to the PM shall also be identified. Any limitations on delivery to, or use by, the PM of supplier-prepared specifications shall be stated. This paragraph shall also identify the software documentation imposed or to be generated as part of the Allocated Baseline.

(b) **Paragraph 3.5.2.2 – Drawings**. This paragraph shall identify the drawings and diagrams that are a part of or shall be a part of the Allocated Baseline. A list of interface control

drawings for both hardware and software shall be described here or in a separate appendix. Plans for the preparation, review, and release of drawings shall be outlined.

(3) **Paragraph 3.5.4 - Product Baseline**. The details of the documents to be utilized in establishing this baseline shall be listed. Plans for preparation, review, release and control of the specifications and drawings and CSCI code standards shall be outlined.

(a) **Paragraph 3.5.4.1 - Specifications**. This paragraph shall identify the hardware and software specifications which the supplier shall prepare to establish the product baseline and the format to which they will be prepared.

(b) **Paragraph 3.5.4.2 - Drawings and Associated Lists**. This paragraph shall define the drawings practices for application to the CI. Any limitation on delivery to, or use by the PM, of supplier-prepared drawings shall be stated. The use of interface control drawings and the identification of interface parameters shall be addressed.

g. **Paragraph 3.6 - Documentation library**. The supplier shall establish a CI documentation library and implement procedures for controlling the documents residing within the documentation library.

h. **Paragraph 3.7 - Drawing library**. The supplier shall establish a drawing library and implement procedures for controlling the drawings, computer aided design (CAD), and computer aided manufacturing (CAM) instructions residing within the drawing library.

i. **Paragraph 3.8 - Software Development Library**. The supplier shall establish a software development library (SDL) and implement procedures for controlling and safeguarding the software residing within the SDL.

j. **Paragraph 3.10 - Engineering Release System**. In this paragraph the supplier shall describe his plans to ensure that engineering data shall be released or processed through a central authority to ensure coordinated action and to preclude unilateral release of data.

(1) **Paragraph 3.10.1 - Engineering Release Record**. In this paragraph the supplier shall describe his plans to ensure that each engineering release record (supplier, subsupplier, or vendor supplied) shall contain:

(a) the CI number and serial numbers (if applicable) of the items affected; and

(b) for each document listed, the document number, title, NSCM number, number of sheets, date of release, revision index and the engineering change number, if applicable.

Configuration Control. This section shall define the responsibilities and procedures used within the supplier's organization for configuration control of established CI, and for processing changes to these CI. The authority and

responsibility of the supplier and the PM with respect to configuration control shall be defined herein.' Plans for reconciling the software status reports and the status of the software, and the technical documentation with the approved baselines (including approved changes) shall be also addressed.

a. **Paragraph 4.1 - Configuration Control Board (CCB)**. This paragraph shall describe the authority and responsibility of the supplier's CCB, including the authority of the CCB for change authorization (i.e., Recommendation or
Action);

b. **Paragraph 4.2 - Configuration Change Procedures**. This paragraph shall address:

(1) for changes that affect established baselines, the formatting, processing and submitting of Engineering Change Proposals (ECP) in combination with Notice of Revisions (NOR), and Requests For Deviations/ Requests For Waivers (RFD/RFW) shall be described;

(2) internal procedures for processing changes which do not affect established baselines and rest within supplier authority. Copies of the suppliers forms as exhibits shall be included along with the narrative;

(3) procedures for ensuring implementation of approved changes into configuration identification, production, spare parts, retrofit and technical publications programmes. Procedures to ensure feedback to the PM shall be described; and

(4) the inputs to the status accounting system shall be clearly defined and linked to the change process. Capabilities for the monitoring of changes shall be described in detail.

c. **Paragraph 4.3 - Part Substitution**. The supplier shall describe a procedure for parts substitution and obtain approval by the customer.

d. **Paragraph 5.1 - Interface Management**. This section shall describe the documentation and control of all physical and functional interfaces of systems, equipment, software, facilities and installation requirements. The criticality of maintaining interfaces may require an intensive interface management program which may be administered separately from the CM program. If such a program is required, the CMP shall describe that program, e.g., charters, working groups, etc. If a separate interface management program is not required, the CMP shall detail how the identification and control of the interfaces shall be accomplished.

(1) **Paragraph 5.1.1 - Documentation**. This paragraph shall specify the documentation to be generated as part of the interface control. The documents shall be listed by type, e.g., drawings and specifications with titles and dates. Also plans to identify interface parameters on the production documentation shall be specified.

(2) **Paragraph 5.1.2 - Interface Control**. This paragraph shall describe the authority, responsibilities, and procedures for releasing and revising the interface control documents.

(3) **Paragraph 5.1.3 - Interface Control Working Group (ICWG)**. The supplier shall describe the establishment and participation in the
Interface Control Working Group (ICWG).

e. **Paragraph 6.1 - Configuration Status Accounting and Configuration data management**. The Supplier shall outline his plan for status accounting and technical data management.

(1) **Paragraph 6.1.1 – Configuration Data Handling**. The supplier shall describe his methods for collecting, recording, processing and maintaining data necessary to provide an adequate configuration data management and status accounting.

(2) **Paragraph 6.1.2 - Reporting**. The supplier shall recommend as a minimum the following reports, to the PM for approval, adequate to:

(a) Identify the current approved configuration documentation and configuration identifiers associated with each CI;

(b) Status of proposed engineering changes from initiation to implementation;

(c) Results of configuration audits, status, Action items and disposition and discrepancies;

(d) Status of deviations and waivers;

(e) Traceability of changes from baseline documentation of each
CI; and

(f) Effectivity and installation status of configuration changes to all CI at all locations.

(3) **Paragraph 6.1.3 – Configuration Data access**. The supplier shall describe methods of accessing the information and/or frequency of reporting and distribution.

(4) **Paragraph 6.1.4 – Configuration Management (CM) Metrics**. The supplier shall describe his methods of measuring the CM process, schedule of regular reports, as required, to the PM, and process descriptions that will lead to compliance with:

(1) The supplier shall establish and implement a configuration management process that shall be used to control the documentation and repositories/libraries containing the elements of the configuration.

(2) The supplier shall prepare a problem/change report to describe each problem detected in software or documentation that has been placed under internal configuration control. The problem/change report shall describe the corrective action needed and the actions taken to resolve the problem. These reports shall serve as input to the corrective action process.

(3) The supplier shall implement a corrective action process for handling all problems detected in the products under internal configuration control. The corrective action process shall ensure that all detected problems are promptly reported, action is initiated on them, resolution is achieved, status is tracked and reported, and records of the problems are maintained for the life of the contract.

f. **Paragraph 7.1 - Configuration Audits**. This section shall describe:

(1) plans, procedures and documentation, for the conduct of the Functional and Physical Configuration;

(2) the format for reporting results of configuration audits; and

(3) schedule periods and agendas for the conduct of CM audits.

g. **Paragraph 8.1 - Technical Reviews**. Suppliers shall describe schedules for and the degree of participation of CM personnel in technical reviews.

REFERENCE # 4.3.D - Derived from MIL-STD-973)

The Supplier's CMP shall comply with the requirements below:

A.1 GENERAL

A.1.1 Scope. This Appendix contains recommendations for the format and content preparation for the CM Plan as described in Paragraph 5.2.

A.1.2 Applicability. The provisions of this Appendix apply whenever the supplying activity is required to prepare a CM plan. The acquiring activity may develop a CM Plan to outline the overall CM approach and as a guide in the development of the supplying activity's CM Plan.

A.2 REQUIREMENTS FOR A CONFIGURATION MANAGEMENT PLAN

A.2.1 Content and format. The configuration management plan shall address the content described in this Appendix as applicable. The format of the plan is at the discretion of the supplying activity or as required by the contract.

A.2.2 Cover Page. This page contains the document control number and revision in the upper right-hand corner. In the center of the page, these words appear in the following format:

CM PLAN
FOR THE
[Project Name or CI nomenclature and number]

CONTRACT NO. [contract number]

CDRL SEQUENCE NO. [CDRL number]

[Date of document - day month year]

Prepared for:
[Contracting Agency Name, Department Code]

Prepared by:
[Contractor name and address]
[CAGE code]

A.2.2.1 Record of Review and History page. This page includes the review and approval dates of all changes to the plan.

A.2.2.2 Table of Contents. The Table of contents lists the title and page number of all titled paragraphs and subparagraphs. The Table of contents then list the title and page number of all Figures, Tables, and Appendices, in that order.

A.2.2.3 Section 1. Introduction. This section includes the project description, purpose of CM Plan, scope and specific contractual applicability of the CM Plan to the project.

A.2.2.4 Section 2. Organization. This section describes the configuration management organization, authority, and the relationship between organizations.

A.2.2.5 Section 3. Configuration Management Phasing and Milestones. This section describes and graphically portray the events and milestones for implementation of CM in phase with major program milestones and events.

A.2.2.6 Section 4. Data Management. This section describes the methods for meeting the configuration management technical data requirements under the requirements of the contract. (See 4.3)

A.2.2.7 Section 5. Configuration Identification. This section describes the supplying activities' procedures for meeting the requirements of section 5.3, including:

a. Selection of CIs;

b. Establishment and management of developmental configuration including document, MBD datasets, drawing and software development libraries and corrective action process;

c. Establishment of the Functional, Allocated and Product baselines, definition of the configuration documentation required for each and graphic illustration of configuration documentation relationships;

d. Assignment and application of configuration identifiers including document numbers, nomenclature, serial numbers and part number to hardware; and software identifiers to software and firmware.

A.2.2.8 Section 6. Interface management. This section describes the procedures for identification of interface requirements, establishment of interface control documents (ICDs) and participation in interface control working groups (ICWG).

A.2.2.9 Section 7. Configuration Change Management. This section describes the supplying activities' procedures for meeting the requirements of 5.4, including:

a. Designation and responsibility of the Configuration Change Authority;

b. Functions, responsibility, and authority of configuration control boards;

c. Classification and priority of changes, and the level of authority for change approval/concurrence;

d. Processing of Requests for Variances; Engineering Change Proposals, Value Engineering Change Proposals and Notices of Revision.

e. Processing of Engineering Release Records.

A.2.2.10 Section 8. Configuration status accounting. This section describes the supplying activities' procedures for meeting the requirements of Section 5.5 and Appendix H, including:

a. The supplying activities' methods for collecting, recording, processing and maintaining

data necessary to provide contractual status accounting information via reports and/or database access;

b. Description of reports/information system content related to, as applicable:

(1) Identification of current approved configuration documentation and configuration identifiers associated with each CI;

(2) Status of proposed engineering changes from initiation to implementation;

(3) Results of configuration audits; status and disposition of discrepancies;

(4) Status of requests for critical and major variances;

(5) Traceability of changes from baselined documentation of each CI; and

(6) Effectivity and installation status of configuration changes to all CIs at all locations.

c. Identifying methods of access to information in status accounting information systems and/or frequency of reporting and distribution.

A.2.2.11 Section 9. Configuration audits. This section describes the supplying activities' approach to meeting the requirements of Section 5.5, including plans, procedures, documentation, and schedules for functional and physical configuration audits; and format for reporting results of in-process configuration audits.

A.2.2.12 Section 10. Subcontractor control. This section describes the methods used by the supplying activity' to ensure subcontractor compliance with configuration management requirements.

A.2.3 Section 11. Other requirements. The following requirements shall also be addressed:

a. Personnel: Number and skills of configuration management staff.

b. Facilities: Administrative space, records storage and office equipment.

c. Information Systems: File servers and communication bandwidth to support internal and external users, internet/intranet access and control, back-up systems.

d. CM Tools: Project Data Management applications, software development tools and authoring software for drawings, MBD datasets, specifications and manuals.

e. Data Deliverables: Specifications, standards, MBD datasets, drawings, reports, and TDPs required as deliverables.

NATO STANDARD

ACMP-2100

THE CORE SET OF CONFIGURATION MANAGEMENT CONTRACTUAL REQUIREMENTS

Edition A Version 2
MARCH 2017

NORTH ATLANTIC TREATY ORGANIZATION

ALLIED CONFIGURATION MANAGEMENT PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

6 March 2017

1. The enclosed Allied Configuration Management Publication ACMP-2100, THE CORE SET OF CONFIGURATION MANAGEMENT CONTRACTUAL REQUIREMENTS, Edition A, Version 2, which has been approved by the nations in the Life Cycle Management Group (AC/327), is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 4427.

2. ACMP-2100, Edition A, Version 2 is effective upon receipt and supersedes ACMP-2100, Edition A, Version 1 which shall be destroyed in accordance with the local procedure for the destruction of documents.

4. This publication shall be handled in accordance with C-M(2002)60.

Edvardas MAŽEIKIS
Major General, LTUAF
Director, NATO Standardization Office

RESERVED FOR NATIONAL LETTER OF PROMULGATION

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS

Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.

INTENTIONALLY BLANK

RECORD OF SPECIFIC RESERVATIONS

[Nation]	[detail of reservation]

Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.

INTENTIONALLY BLANK

TABLE OF CONTENTS

FOREWORD VIII

CHAPTER 1 GENERAL 1
1.1. Purpose 1
1.2 Composition of requirements in ACMP-2100 1
1.3 Applicability 2
1.4 Compliance with this publication 2

CHAPTER 2 REFERENCES 3
2.1. Normative references 3
2.2. Informative references 3

CHAPTER 3 TERMS AND DEFINITIONS 5
3.1. ISO 10007 Terms and Definition applies 5
3.2. Additional NATO terms, definitions and notes 5

CHAPTER 4 REQUIREMENT FOR CONFORMANCE TO ISO 10007 7
4.1 Specific changes to the ISO 10007 wording 7
4.2 General changes to the ISO 10007 wording 7

CHAPTER 5 NATO SPECIFIC REQUIREMENTS 9
5.1. Requirements for Sub-suppliers 9
5.2. Configuration Management Planning 9
5.3. Product Configuration Information 9
5.4. Change Control 9

FOREWORD

Configuration Management (CM) is a critical process for NATO lifecycle management. This publication defines the core CM requirements for Suppliers in all lifecycle stages. It is a NATO adoption of ISO 10007:2003[1], supplemented by additional NATO requirements in Chapter 5, and is entirely applicable in all NATO programmes (thus denoted “core CM requirements”). If the requirements provided in this publication are found insufficient to meet the actual needs for all Life Cycle stages of the programme, further CM requirements may be defined and added to the contract by using the corresponding guidance on CM.

This publication has been developed to provide Acquirers with means to contractually invoke core Configuration Management requirements within NATO multinational joint projects and National programmes during the product Life Cycle.

CM helps to assure that the product design will be consistent with the Acquirer’s requirements and that product and system interfaces remain compatible; including spares, test equipment, tools, ancillaries and supporting documentation. Effective CM provides a framework to ensure that all users are kept informed of currently approved/released configuration information.

Configuration management documents the product’s configuration. It provides identification and traceability, the status of achievement of its physical and functional requirements, and access to accurate information in all stages of the Life Cycle.

Configuration baselines are established by defining materiel, both functionally and physically, by means of drawings, specifications and other relevant data and documentation.

The term “product” in this publication should be interpreted as applicable to the generic product categories; e.g., documents, facilities, firmware, hardware, software, tools, materials, processes, services, systems.

Configuration Management (CM)[2] applies appropriate processes and tools to establish and maintain consistency between the product and the product requirements and attributes defined in product configuration information. A disciplined CM process ensures that products conform to their requirements and are identified and documented in sufficient detail to support the product Life Cycle. CM assures accurate product configuration information and enables product interchangeability and safe product operation and maintenance to be achieved.

[1] Whenever “ISO 10007” is used in this publication text, it refers to ISO 10007:2003.
[2] Source: GEIA-HB-649

CHAPTER 1 GENERAL

ACMP-2100 contains the NATO core set of contractual requirements for Configuration Management. A system needs to be established, documented, applied, maintained, assessed and improved, and/or evaluated, in accordance with requirements contained in the subsequent sections.

1.1. Purpose

1. This publication contains the set of core CM requirements, which if applied appropriately, can provide confidence in the Supplier's capability to deliver products that conform to Acquirer's contract requirements.

2. The responsibilities and authorities for CM are at first outlined, before describing the configuration management process that includes configuration management planning, configuration identification, change control, configuration status accounting and configuration audit.

1.2 Composition of requirements in ACMP-2100

1. The NATO requirement for an ISO 10007 based CM process and any applicable changes or deletions of ISO content is defined in Chapter 4 of this publication:

   a. "Specific Change": a change to one or more words, a sentence and/or section of the ISO 10007 text (shown with *italic letters*).

   b. "General Change": a replacement of one or more words throughout the ISO 10007 to turn the text into contractual requirement(s).

2. Additional NATO specific requirements are defined in Chapter 5 of this publication.

1.3 Applicability

1. This publication is primarily intended for use in a contract between two or more parties.

2. When referenced in a contract, this publication shall apply to all of the processes necessary for the Supplier to fulfil the contractual requirements.

3. This publication may also be used internally by a Supplier or a potential Supplier to cover the Configuration Management aspects of the Management System (MS).

4. Where identified by the Acquirer, this publication can be used in conjunction with other appropriate standards to manage processes of the MS.

5. Order of precedence
If inconsistencies exist between the contract requirements and this publication, the contract requirements shall prevail. In the event of a conflict between the text of this publication and the references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

1.4 Compliance with this publication

1. Compliance with this publication for a contract is defined as the fulfilment of the requirements of Chapters 4 and 5.

2. In this publication, NOTEs are not contractual requirements.

CHAPTER 2 REFERENCES

2.1. Normative references

The following referenced documents are indispensable for the application of this publication. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

1. ISO 9000 Quality management systems – Fundamentals and vocabulary
2. ISO 10007:2003 Quality management system – Guidelines for configuration management

2.2. Informative references

1. STANAG 4427 Configuration Management in System Life Cycle Management
2. ANSI/EIA-649 Configuration Management Standard
3. MIL-HDBK-61 Military Handbook, Configuration Management Guidance
4. DEF STAN 05-57 Configuration Management of Defence Material
5. prEN 9223 part 100 through 105 Programme Management – Configuration Management

INTENTIONALLY BLANK

CHAPTER 3 TERMS AND DEFINITIONS

3.1. ISO 10007 Terms and Definition applies

3.2. Additional NATO terms, definitions and notes

1. Concession

NOTE A:
Concessions are not to be confused with approved alternates or substitutes, which are in the configuration baseline.

2. Dispositioning Authority

NOTE A:
NATO considers the Dispositioning Authority to be a person who may be supported by a CCB, which is not mandatory unless stated in the contract.

3. Acquirer

A governmental or NATO organization that defines the requirements for the delivery of a product by a supplier and enters into a contractual relationship with that supplier.

Note:
The acquirer is often known by a variety of names like owner, buyer, stakeholder, requirer, project management office, purchaser, customer, etc.

4. Product

Examples: document; facility; firmware; hardware; software; tool; material; process; service; system.

5. Release

A configuration management action whereby a particular version of a product or product configuration information is made available for a specific purpose.

6. Supplier

An organization that acts in a contract as the provider of products to the acquirer.

Notes:

The supplier is often known by a variety of names like contractor, producer, seller, or vendor.

Sometimes the acquirer and the supplier are part of the same organization.

INTENTIONALLY BLANK

CHAPTER 4 REQUIREMENT FOR CONFORMANCE TO ISO 10007

A Configuration Management system shall be established, documented, applied, maintained, assessed and improved, and/or evaluated, in accordance with ISO 10007, incorporating the following changes to the ISO 10007.

4.1 Specific changes to the ISO 10007 wording

Changes shown with *italic letters.*

ISO 10007 paragraph 5.2 Configuration management planning

- Change last line to:

Annex A of ISO 10007 describes a potential structure and content for a configuration management plan*, and is only informative*.

ISO 10007 paragraph 5.3.2 Product configuration information

- Change first paragraph to:

Product configuration information comprises both product definition and product operational information. This typically includes requirements, specifications, design drawings, parts lists, software documents and listings, models, *markings, audit information, effectivity,* test specifications, maintenance and operating handbooks.

4.2 General changes to the ISO 10007 wording

Whenever the ISO 10007 uses the word “should” or “may” in section 4 and 5, it is to be read as “shall”, and compliance by the Supplier is mandatory, unless otherwise determined by the Acquirer.

Whenever the ISO 10007 uses the phrase “Life Cycle of the product”, it is to be read “contract”.

INTENTIONALLY BLANK

CHAPTER 5 NATO SPECIFIC REQUIREMENTS

5.1. Requirements for Sub-suppliers

1. The Supplier shall consign the applicable contractual configuration management requirements to its Sub-suppliers by referencing the stated contractual requirement.

2. The supplier shall ensure that the procedures and processes required to fulfil contract requirements are fully implemented at the sub-suppliers facilities.

5.2. Configuration Management Planning

1. The Supplier shall provide access to the Configuration Management Plan (CMP) to the Acquirer.

2. The Acquirer reserves the right to reject the CMP.

3. The Supplier shall define the CM organization and its relation to the overall organization in the CMP.

5.3. Product Configuration Information

1. As a minimum, for each CI, the Supplier shall develop and maintain configuration information.

2. As a minimum the Supplier shall include the NCAGE in the information related to the CI(s).

3. The Supplier shall only use configuration information that has been formally released.

4. Configuration Information shall take into account any access limitations; as a minimum, Security classifications and proprietary license constraints.

5.4. Change Control

1. The Supplier assumes total risk for the implementation of changes incorporated prior to approval by the Dispositioning Authority.

ACMP-2100(A)(2)

SUPREME HEADQUARTERS ALLIED POWERS EUROPE
GRAND QUARTIER GÉNÉRAL DES PUISSANCES ALLIÉES EN EUROPE
Mons - Belgium

SH/SEM/J2/X/SPO/JNW/21-009330/1 22 December 2021

ACO DIRECTIVE 070-001

ALLIED COMMAND OPERATIONS SECURITY DIRECTIVE

REFERENCES:
A. AD 070-001, ACO Security Directive, dated 28 January 2019.
B. C-M(2002)49-REV1, Security within the North Atlantic Treaty Organization (NATO), dated 20 November 2020.
C. AC/35-D/2000-REV8, Directive on Personnel Security, dated 25 November 2020.
D. AC/35-D/2001-REV3, Directive on Physical Security, dated 25 November 2020.
E. AC/35-D/2002-REV5, Directive on the Security of NATO Classified Information, dated 25 November 2020.
F. AC/35-D/2006, Directive for NATO on Security in Relation to Non-NATO Entities, dated 26 November 2020.
G. AC/35-D/1029-REV2, Supporting Document on Security Education and Awareness, dated 22 January 2021.

1. **Status.** This directive supersedes the Allied Command Operations (ACO) Directive (AD) 070-001 dated 28 January 2019.

2. **Purpose.** The purpose of this revision is to incorporate recent changes in NATO Security Policy and supporting documents.

3. **Applicability.** This directive is applicable to all ACO headquarters and units and should be used as a basis for the preparation of local directives.

4. **Publication Updates.** Updates are authorized when approved by the Chief of Staff SHAPE. An assessment for a revision is to be carried out not later than two years after the release date of this publication.

5. **Proponent.** The proponent for this directive is SHAPE SEM J2 X Security Policy and Oversight (SPO) Section.

FOR THE SUPREME ALLIED COMMANDER, EUROPE:

Original signed

Phillip Stewart
Major General, USA AF
Deputy Chief of Staff, Strategic Employment

SHAPE
7010 Mons, Belgium
Office : +32 65 443967
NCN 254-3967
Fax : +32 65 443545 (Registry)
J2XSEC@shape.nato.int

TABLE OF CONTENTS

SUBJECT	PAGE	PARA
PART I – BASIC PRINCIPLES AND ORGANISATION		
CHAPTER 1 – BASIC PRINCIPLES AND MINIMUM STANDARDS		
Introduction	16	1-1
General Terminology	16	1-2
Applicability to Organisations and Commanders	16	1-3
Minimum Standards	16	1-4
Cryptographic Material	16	1-5
ATOMAL Information	16	1-6
Signals Intelligence	16	1-7
Major Principles	16	1-8
Security Organisation	17	1-9
Physical Security	17	1-12
Security of NATO Classified Information	18	1-23
Personnel Security	19	1-32
Communication and Information System Security	19	1-37
CHAPTER 2 – SECURITY ORGANISATION, RESPONSIBILITIES AND PLANNING		
Role of the Military Committee	20	2-1
Security Authority	20	2-2
Delegation of Security Authority	20	2-3
Command Responsibility	20	2-4
Security Appointments	20	2-5
Security Plans and Instructions	22	2-6
Individual Responsibility	23	2-7
Internal Security Reviews	23	2-8
Counter-Intelligence Support	23	2-9
PART II – PHYSICAL SECURITY		
CHAPTER 1 – PHYSICAL SECURITY FOR GENERIC PROTECTION AND TO COUNTER ESPIONAGE AND SUBVERSION		
General Principles	26	1-1
Security Requirements	26	1-2
Security Areas	26	1-3
Security Area Concept	27	1-4
Assessment of Requirements	27	1-5
Administrative Zones	27	1-6
Control of Entry	28	1-7
Visitor Control	28	1-9
Physical Access to NATO Classified Security Areas by Individuals from Non-NATO Entities	28	1-10
Automated Control of Entry Systems	28	1-11
Entry and Exit Searches	29	1-12
Security Passes	29	1-13
Security Guards	29	1-14
Security Guard Patrols and Checks	30	1-15

Guard Response Forces	30	1-16
Intrusion Detection Systems	30	1-17
Minimum Standards for Storage of NATO Classified Information	31	1-18
Security Containers	31	1-19
Vaults and Strong Rooms	31	1-20
Locks	32	1-21
Combination Settings	32	1-22
Security Keys	32	1-23
Office Security	32	1-24
Eavesdropping	33	1-25
Technically Security Areas	33	1-26
Conference Rooms	34	1-27
Counter-Intelligence Technical Security Programme	34	1-28
Electrical Equipment in Security Areas	34	1-29

CHAPTER 2 – PROTECTIVE MEASURES AGAINST TERRORIST AND SABOTAGE THREATS WITHIN NATO COUNTRIES

Introduction	36	2-1
Threats and Risks	36	2-2
Types of Threat	36	2-4
Host Nation Responsibilities	37	2-5
Parent (or Sending) Nation Responsibilities	37	2-9
ACO Component Responsibilities	38	2-12
Scope of Security Protection	38	2-16
Security Planning - Design of Installations	38	2-17
Internal Security Plan	39	2-19
Training and Inspections	40	2-20
Standard NATO Alert System	40	2-21
Receipt of Indications and Warning of Terrorist Activity	40	2-22
Reporting Threats of Terrorist and Sabotage Activities and Declarations of Alert States	40	2-23
Budgeting for Physical Protection and Other Protective Material	41	2-24
Security Staff	41	2-25
Coordination and Monitoring of Counter-Terrorist and Counter-Sabotage Arrangements	41	2-26

CHAPTER 3 – PROTECTIVE MEASURES AGAINST TERRORIST AND SABOTAGE THREATS OUTSIDE NATO COUNTRIES

Introduction	44	3-1
Risks	44	3-2
Threats	44	3-3
Assessing the Threat	45	3-4
Responsibilities	45	3-5
Reporting of Terrorist or Sabotage Activities	46	3-9
Internal Security Plan	47	3-11

PART III – SECURITY OF INFORMATION

CHAPTER 1 – DOCUMENT CLASSIFICATIONS AND MARKINGS

Introduction	52	1-1
Information Sharing	52	1-3
Information Access and Releasability	52	1-4
Consistency of Security Markings	52	1-5
Public Release and Disclosure of NATO Classified Information	52	1-6
Security Classifications	52	1-7
Component Security Markings	53	1-9
Aggregation Principle	53	1-11
Authority to Apply COSMIC TOP SECRET Classification	53	1-12
Change of Classification	53	1-13
Individual Responsibility	53	1-17
Security Markings Applied to NATO Classified Information	54	1-18
Application of NATO Information Markings	55	1-30
Overall Classification	57	1-34
Website Markings	57	1-35
Changes or Additions to Security Markings	57	1-36
Automatic Downgrading/Declassification	57	1-37
Approved Security Markings	57	1-38
Ownership Markings	58	1-40
Classification Markings	59	1-42
Releasability and Dissemination Limitation Markings	60	1-45
Administrative Markings and Category Designators	61	1-47
Definition of Terms	62	1-48

CHAPTER 2 – THE ACO COSMIC TOP SECRET AND ATOMAL REGISTRY SYSTEMS

General	64	2-1
ACO COSMIC TOP SECRET and ATOMAL Registry Systems	65	2-2
ACO Security Authority	68	2-7
Dissemination of CTS and ATOMAL information within ACO	68	2-8
Dissemination of CTS and ATOMAL information between ACO and Other NATO Components	69	2-9
Control of COSMIC TOP SECRET and ATOMAL Documents	69	2-10
Page Checking	70	2-11
Classification of ATOMAL information	70	2-12
Marking of Documents	71	2-13
Personnel Security Clearances	72	2-14
Access	72	2-15
Disclosure Record	72	2-16
Accountability	73	2-17
Reproductions	73	2-18
Generated Documents	73	2-19
Oral and Visual Communications	73	2-20
ATOMAL Exercise Documents	74	2-21
Disposition	74	2-22

Security Briefings	74	2-23
Reports	75	2-24
Inspections	75	2-25
Breaches of Security and Compromises	75	2-26
Responsibilities	76	2-27

CHAPTER 3 – PREPARATION, TRANSFER, CONTROL AND DESTRUCTION OF CLASSIFIED DOCUMENTS

Preparation and Display of Security Classifications and Markings	81	3-1
Reclassification Marking Procedures	82	3-2
Aural and Visual Projections of Classified Material	82	3-3
File Reference Numbers	83	3-4
Dating and Copy Numbering	83	3-5
Page Numbering and Page Count Details	83	3-6
Additional Copies and Translations	83	3-7
Microfilming and Reproduction from Microfilm	85	3-17
Transfer of NATO Classified Material	86	3-18
Hand Carriage	86	3-21
Couriers/Guards/Escorts	86	3-22
Internal Transfer within Establishments of ACO Components	86	3-23
Transfer outside of ACO Component Establishment within a NATO Nation	87	3-24
Transfer between the Territories of NATO Nations	87	3-27
NATO Seals and Courier Seals	89	3-34
Special Transmission Procedures	89	3-35
Control of Classified Documents	90	3-36
Disclosure Control Records for COSMIC TOP SECRET and Certain ‘Special Limitations’ Documents	91	3-37
Control Numbers – COSMIC and ATOMAL Documents	92	3-38
Accountability	92	3-39
Receipt and Page Numbering of NATO Classified Material	92	3-40
Page Checking	92	3-41
Receipts for NATO CONFIDENTIAL/NATO RESTRICTED	92	3-42
Control of Classified Working Papers	92	3-43
Changes to NATO Classified Documents	94	3-44
Physical Musters and Spot Checks	94	3-46
Handover/Transfer Procedures	94	3-47
Destruction	94	3-48
Destruction Certificates	95	3-49

CHAPTER 4 – RELEASE OF NATO CLASSIFIED INFORMATION TO NON-NATO RECIPIENTS

Introduction	97	4-1
General Requirements	97	4-2
Security Agreements and Administrative Arrangements	97	4-4
Security Assurances	98	4-6
Sponsorship by a NATO Nation	98	4-8
Release Authority	99	4-13
Principles for Authorising the Release of NATO Classified Information	100	4-17

Administrative Arrangements for the Implementation of a Security Agreement	102	4-19
Classification Marking System	102	4-20
Security Arrangements for the Release of NATO Classified Information to Non-NATO Nations, International Organisations and Personnel on Partnership Staff Posts	103	4-21
NATO Office of Security Certification	103	4-22
Access to NATO Classified Information by Partner Officers on Partnership Staff Posts	103	4-23
Records of Release Information	104	4-24

PART IV – PERSONNEL SECURITY

CHAPTER 1 – ACCESS TO NATO CLASSIFIED INFORMATION

Introduction	107	1-1
Personnel Security Clearance (PSC)	107	1-2
Personnel Security Clearance Confirmation (PSCC)	108	1-6
Responsibilities	108	1-11
Security Briefings	110	1-17
Interim or Temporary PSCs	111	1-24
Provisional Appointments	112	1-25
Administration of PSCs	112	1-27
Access to NATO Classified Information	112	1-31
Access to COSMIC TOP SECRET Information	113	1-33
Access to ATOMAL Information	113	1-34
Access to NATO Crypto Information	113	1-35
Temporary Access	113	1-36
Senior Government Officials	114	1-38
Contractor Personnel	114	1-39
Interpreters	114	1-40
Emergency Access	114	1-41
Access to NCI by Integrated Members	115	1-43
Insider Threat	115	1-46
Reporting Adverse Personnel Matters	116	1-49
Removal of Personnel from Post	116	1-50

CHAPTER 2 – SECURITY EDUCATION AND AWARENESS

General Principles	118	2-1
Knowledge of Security Instructions	118	2-2
Security Awareness Officers	118	2-3
Responsibilities	118	2-4
Objectives of Security Education and Awareness	118	2-5
Methods of Security Education and Awareness	119	2-6
Security Awareness Programme Content	121	2-7
Newcomer Activities	121	2-8
Continuous Security Education and Awareness	121	2-9
Breaches of Security	121	2-10
Quarterly Security Returns	122	2-11
Training of Security Officials	122	2-12

CHAPTER 3 – TRAVEL SECURITY

Temporary Duty Travel	124	3-1
Private Travel	124	3-3

PART V – COMMUNICATION AND INFORMATION SYSTEM SECURITY

This Part has been removed to separate ACO Directive AD 070-005

PART VI – SECURITY PROCEDURES

CHAPTER 1 – SECURITY INCIDENTS

General	130	1-1
CIS Security Breaches	130	1-2
Definitions	130	1-3
Investigative Procedures	130	1-7
Role of the Principle/Command Security Advisor	132	1-11
Reporting Procedures	132	1-12
Remedial Actions	134	1-20
Confirming Authority	134	1-21
Records of Security Breaches	134	1-22
Investigative Policy	135	1-23

CHAPTER 2 – SECURITY INSPECTIONS

ACO Security Inspections	136	2-1
Inspection Responsibilities	136	2-3
Frequency of Inspections	136	2-5
Security Advisory Visits (SAV)	137	2-7
Methodology	137	2-8
Reporting Procedures	139	2-18

PART VII – CLASSIFIED PROJECT AND INDUSTRIAL SECURITY

CHAPTER 1 – INTRODUCTION

General	142	1-1
Scope	142	1-3
Definitions	142	1-4
Authority	143	1-5

CHAPTER 2 – TENDERING, NEGOTIATION AND LETTING OF CONTRACT/SUB-CONTRACTS INVOLVING NATO CLASSIFIED INFORMATION

Contracts/Sub-Contracts in NATO Nations – General	144	2-1
Tendering Process	144	2-3
Unsuccessful Bidders	146	2-5
Negotiations	146	2-6
Contracts	146	2-9
Performance of Contracts within ACO Component Class II Security Areas	146	2-12
Programme/Project Security Instruction (PSI) and Security Aspects Letter (SAL)	147	2-13
Notification of Contracts	147	2-16

Contracts/Sub-Contracts with Contractors in Non-NATO Nations	148	2-23
Termination of Contracts involving Classified Information	148	2-28
CHAPTER 3 – INDUSTRIAL SECURITY CLEARANCES		
Facility Security Clearances	149	3-1
Contractor Personnel Performing Work on ACO Component Premises or on Other Contractor Facilities	150	3-9
Changes to or Revocation of FSC	150	3-10
CHAPTER 4 – FACILITY SECURITY OFFICER		
General	151	4-1
Responsibilities	152	4-3
CHAPTER 5 – PERSONNEL SECURITY CLEARANCES		
General Provisions	153	5-1
Contractual Conditions	153	5-4
Initiating Personnel Security Clearance Procedures	153	5-5
Renewal of PSCs	153	5-6
PSC of an Employee Holding the Nationality/Citizenship of Another Nation	153	5-8
Multiple Nationalities	154	5-11
Provisional PSCs	154	5-12
Confirmation of PSCs	154	5-14
Security Awareness and Briefings of Individuals	154	5-15
Procedures to be Followed When a PSC is Altered, Suspended or Revoked	155	5-18
Procedures to be Followed When a PSC is Denied	155	5-22
CHAPTER 6 – PROGRAMME/PROJECT SECURITY		
Introduction	157	6-1
Security-by-Design	157	6-2
Programme/Project/Construction Security Instructions	157	6-3
Principles	157	6-6
CHAPTER 7 – RELEASE OF NATO CLASSIFIED INFORMATION BY PROGRAMME/PROJECT PARTICIPANTS AND CONTRACTORS/SUB-CONTRACTORS		
Security Arrangements for the Release of NCI to Non-NATO Entities	161	7-1
CHAPTER 8 – HANDLING OF NATO CLASSIFIED INFORMATION IN COMMUNICATION AND INFORMATION SYSTEMS		
General	163	8-1
Security Accreditation Process	163	8-9
Security-Related Documentation	164	8-10
Interconnection of CIS	164	8-11
CHAPTER 9 – INTERNATIONAL VISIT CONTROL PROCEDURES		
Requirements and Procedures for Visits	165	9-1

CHAPTER 10 – INTERNATIONAL TRANSFER AND TRANSPORTATION OF NATO CLASSIFIED INFORMATION AND MATERIAL

General	167	10-1
Transfer by International Hand Carriage of NATO Classified Material at NC or NS Level	167	10-3
Security Arrangements	167	10-4
Procedure	167	10-7
Transfer of Information at the level NATO CONFIDENTIAL by Non-Security Cleared Commercial Courier Companies (CCC)	168	10-11
Transfer of Information Classified NATO CONFIDENTIAL or NATO SECRET by Transport as Freight	169	10-12
Transfer of Information Classified NATO CONFIDENTIAL or NATO SECRET by Transportation as Freight by Road	169	10-15
Transfer of Information Classified NATO CONFIDENTIAL or NATO SECRET by Transportation as Freight by Rail	170	10-16
Transfer of Information Classified NATO CONFIDENTIAL or NATO SECRET by Transportation as Freight by Sea	170	10-18
Transfer of Information Classified NATO CONFIDENTIAL or NATO SECRET by Transportation as Freight by Aircraft	171	10-19
Security Principles Applicable to all Forms of Transportation	172	10-22
Customs	172	10-23
Acknowledgement	172	10-25
Packaging	172	10-26
Security Guards and Escorts	172	10-27
Transportation of Explosives, Propellants or Other Dangerous Substances	173	10-33

CHAPTER 11 – GLOSSARY AND ACRONYMS

Glossary and Acronyms	175

PART VIII – ACO SECURITY FORMS

This Part has been removed to Enterprise Document Management System.

ANNEXES

A. Physical Protection / Minimum Standards.
B. Storage of NATO Classified Material.
C. Technical Security.
D. TSA Facility Profile.
E. Security Alert States and Countermeasures.
F. Planning Notes for Protection against Attack.
G. Special Limitations for Access to NATO Nuclear Planning Documents.
H. List of the ATOMAL Central Registries which will Act as Central Controlling Office for the ATOMAL Programme in Each NATO Component.
I. Cover Sheet for ATOMAL Documents.
J. Requests for ATOMAL Information.
K. Methods and Criteria for Destruction.
L. Disposal and Destruction of Classified Magnetic Media.
M. Security Assurance.
N. General Procedures for Release of NATO Classified and Unclassified Information to Non-NATO Recipients.
O. Minimum Standards for Handling and Protection of NATO Classified Information up to NATO SECRET to be Met by Non-NATO Recipients.
P. Security Arrangements for the Release of NATO Classified Information to the European Union.
Q. Request for Personnel Security Clearance Confirmation.
R. Personnel Security Clearance Confirmation.
S. NATO International Visit Control Procedures (IVCP).
T. Briefing on Procedures for Safeguarding COSMIC TOP SECRET and ATOMAL Information.
U. Personnel Security Clearance Confirmation (for Non-NATO Citizens).
V. Security Awareness Programme Content.
W. Quarterly Security Return.
X. Security Procedures for Phase I – Evaluation of Security Incident.
Y. Security Procedures for Phase II – Investigation of a Breach of Security.
Z. Security Procedures for Phase III – Reporting of Compromise.
AA. Breach of Security – Initial Report.
BB. Breach of Security – Final Report.
CC. ACO Security Inspection Checklist.
DD. Report of Inspection of Security Arrangements for Protection of NATO Classified Material.
EE. General Responsibilities
FF. Facility Security Clearance Information Sheet (FSCIS).
GG. Contract Security Clause.
HH. Security Aspects Letter (SAL).
II. Facility and Personnel Security Clearance for Contracts Involving NATO Restricted Information National Requirements.
JJ. Project Security Instruction – Structure and Content.
KK. Facilities / Organisations List.
LL. International Visits Processing Times / Lead Times and NATO UNCLASSIFIED or NATO RESTRICTED Notification Requirements.
MM. Security Acknowledgement in Case of Hand Carriage.
NN. Courier Certificate.
OO. International Transportation Plan.

PP. Authorisation for Security Guards.
QQ. Abbreviations.

This page is intentionally left blank.

PART I

BASIC PRINCIPLES AND ORGANISATION

CHAPTER 1: Basic Principles and Minimum Standards

CHAPTER 2: Security Organisation, Responsibilities and Planning

This page is intentionally left blank.

CHAPTER 1 – BASIC PRINCIPLES AND MINIMUM STANDARDS

1-1. **Introduction.** The North Atlantic Council (NAC) has approved the 'Agreement Between the Parties to the North Atlantic Treaty for the Security of Information' which thereby establishes the NATO Security Policy. In turn, this document lays down the basic principles and minimum standards of security to be applied throughout Allied Command Operations (ACO). The principles and minimum standards have been agreed by the NATO Nations so that each may be assured that a common standard of protection is established in each Nation and in every command, agency and formation so that classified information can be shared with confidence.

1-2. **General Terminology.** Throughout this document, the term "shall" denotes a mandatory requirement whilst "should" indicates a strong recommendation to ACO commanders if they are to achieve optimum security standards and the associated protection of NATO Classified Information (NCI). Elements of security also contribute to the wider protective effect which is covered by the ACO Directive (AD) 080-025, ACO Force Protection (FP).

1-3. **Applicability to Organisations and Commanders.** This directive is applicable to all Organisations within ACO. The term "organisation" in relation to this directive includes any formation whether headquarters, centre, agency, unit or element, which is subordinate to Supreme Allied Commander, Europe (SACEUR). The term "commander" means the officially designated head of an organisation, whether military or civilian.

1-4. **Minimum Standards.** This directive is based on the minimum standards agreed by the nations. Subordinate formations should not vary these standards unless in exceptional circumstances.

1-5. **Cryptographic Material.** Detailed regulations relating to cryptographic material and TEMPEST are contained in various communications security (COMSEC) publications in addition to this directive. The provisions of this directive and the COMSEC directives and publications are mutually supportive and are to be applied where appropriate. In case of perceived incompatibility of regulations, the matter shall be referred to the SHAPE SEM J2X Information Assurance (IA) section who will resolve the matter with ACO COMSEC.

1-6. **ATOMAL Information.** Access to, and the protection of, ATOMAL information are subject to the Agreement between the Parties to the North Atlantic Treaty for Cooperation regarding Atomic Information (C-M(64)39). The Administrative Arrangements to implement the Agreement between the Parties to the North Atlantic Treaty for Cooperation regarding ATOMAL Information – the current version of C-M(68)41 – shall form the baseline to control access, handle and protect such information.

1-7. **Signals Intelligence.** The sensitive nature of Signals Intelligence (SIGINT) information, operations, sources and methods require the application of stringent security regulations and procedures often beyond those set forth in this directive. Therefore, access to, and protection of, SIGINT information, operations, sources and methods are subject to national regulations and the provisions laid down in MC 0101 (NATO Signals Intelligence Policy) and its companion Allied Joint Publication (AJP).

1-8. **Major Principles.** The measures of security adopted in each ACO formation must embrace Security Organisation, Physical and Personnel Security, Security of NCI, and Communication and Information System (CIS) Security, all coordinated to meet the

minimum standards and adapted to meet local circumstances and operational requirements. The measures adopted in each ACO formation must extend to all persons having access to NCI and to all premises containing such information or other vital operational assets. This chapter provides a synopsis of the minimum standards to be met in each of the security disciplines; more detailed requirements are found in subsequent chapters.

1-9. **SECURITY ORGANISATION.** Each ACO commander is responsible for security and shall prepare security plans and instructions to implement the requirements of this directive.

1-10. Each ACO commander shall set up a security organisation and shall appoint an officer to exercise staff responsibility throughout the command. Without a properly formed, understood and practised security organisation, the implementation of security policy and measures will be difficult to achieve.

1-11. All personnel assigned to ACO are to be made aware of their individual responsibilities to adopt effective security practices. ACO commanders shall ensure appropriate Security Education and Awareness training programmes are conducted.

ACO COMMANDERS SHALL IMPLEMENT A FORMAL SECURITY INSPECTION PROGRAMME OF SUBORDINATE ELEMENTS, INCLUDING MISSIONS AND OPERATIONS THAT THEY HAVE BEEN ALLOCATED FORMAL OVERSIGHT OVER, RESULTS OF WHICH SHALL BE FORWARDED TO SHAPE SEM J2X AS THE ACO SECURITY AUTHORITY.

1-12. **PHYSICAL SECURITY.** Physical security measures shall be designed to prevent unauthorised access to NCI. Such measures are to be based on the Security Area concept.

1-13. Entry into Security Areas shall be controlled and the system shall be designed to meet the needs of permanent staff, contractors and visitors.

1-14. An effective control of entry system shall require the use of security passes.

1-15. Security Guards shall be properly trained, security cleared and effectively supervised and shall ensure the integrity of Security Areas.

1-16. All NCI shall be stored in approved security containers and the keys and combination settings are to be protected to an equivalent level.

1-17. Each ACO formation shall make arrangements to protect material from overlooking and ensure that NCI is secured when ceasing work or during unsupervised periods.

1-18. Offices in which highly classified information is regularly discussed shall be protected against eavesdropping where the risk warrants it.

1-19. Special installation measures are required to contain the radiation of intelligible signals by equipment that processes classified information by electrical or electronic means. This shall be achieved by TEMPEST zoning of ACO formations.

1-20. All electrical equipment introduced into Security Areas shall be installed in accordance with SDIP-29, Facility Design Criteria and Installation of Electronic Equipment for Processing Classified Information.

1-21. Host Nations (HN) are responsible for the external protection of ACO formations and for keeping ACO commanders informed of the threat.

1-22. In accordance with C-M(2002)50-REV1, ACO commanders are responsible for planning internal security measures to protect their installations and personnel. FP planning considerations should be taken into account to improve operational resilience and to minimise the vulnerability of personnel, facilities, equipment, material, operations and activities from threats and hazards. Greater detail is provided in AD 080-025, ACO Force Protection.

1-23. **SECURITY OF NATO CLASSIFIED INFORMATION.** All ACO formations are to have a registry system for the control of classified documents:

a. COSMIC and ATOMAL documents are to be administered and stored separately.

b. NCI shall be protected throughout its life cycle to a level commensurate with its level of security classification; documents shall remain classified only as long as is necessary.

1-24. ACO commanders are to appoint a COSMIC/ATOMAL Control Officer (CACO) who shall be responsible for the control of COSMIC and ATOMAL information.

1-25. All material shall be classified according to content by the originator; documents are to be marked NATO or COSMIC as appropriate and have the classification prominently displayed. Originators shall consider the potential damage caused by unauthorised disclosure and ensure appropriate classification to generate appropriate safeguarding.

1-26. All ACO formations shall review classified documents at regular intervals for downgrading or destruction. Destruction shall be by approved means.

1-27. Classified documents are to be prepared and transmitted in accordance with the detailed instructions in this directive.

1-28. All material classified COSMIC TOP SECRET, NATO SECRET and ATOMAL information is accountable and the procedures for the control of this material shall be applied rigorously.

1-29. NCI is only to be released outside the Alliance following the procedures contained within the Bi-SC Handbook on Information and Intelligence Sharing (I&IS) with Non-NATO Entities (NNEs) and with the Delegated Authority's (DA) written approval.

1-30. The planning, preparation, execution and support relating to NATO Operations, Training, Exercises, Transformation and Cooperation (OTETC) may require specific additional security aspects to be addressed; the Bi-SC Handbook on I&IS with NNEs contains security provisions and guidance applicable in these circumstances.

1-31. All suspected breaches of security shall be reported as soon as practicable to SHAPE SEM J2X, representing the ACO Security Authority.

1-32. **PERSONNEL SECURITY.** All ACO personnel whose duties require access to information classified NATO CONFIDENTIAL or above are to be cleared before such access is authorised. The clearance procedure is the responsibility of the sending nation who will provide a Personnel Security Clearance Confirmation (PSCC). A NATO Personnel Security Clearance (PSC) is not required for access to NATO RESTRICTED information, although individuals shall be briefed on their responsibilities for the protection of NATO RESTRICTED information.

1-33. Personnel such as messengers, security and cleaning staff shall be cleared to the appropriate level if their duties could result in inadvertent access to NCI.

1-34. Supervisors shall report any incidents, associations or habits likely to have a bearing on the security reliability, or vulnerability, of their subordinates. Personnel who are considered to be at risk shall be removed from positions where they might either endanger operational security or attract a specific personal threat.

1-35. All ACO formations are to maintain records of PSCs, which are to be reviewed regularly to ensure that clearances are current and appropriate to the level of access.

1-36. All ACO personnel should receive security awareness and education training at regular intervals, outlining the threat to security, the need for security and the procedures for achieving it. Advice and guidance can be obtained from SHAPE SEM J2X and assistance sought from Allied Command Counter Intelligence (ACCI) personnel if available.

1-37. **COMMUNICATION AND INFORMATION SYSTEM SECURITY.** ACO commanders are to establish and maintain an effective and appropriate CIS security organisation within their area of responsibility; such that the confidentiality, integrity and continued availability of NATO information, stored, processed or transmitted on CIS, or networks, is ensured. Complete details are published in AD 070-005, ACO Directive on CIS Security.

1-38. ACO Information Security (INFOSEC) Policy shall be applied to all ACO CIS, irrespective of the security classification of the information or data stored or processed thereon.

1-39. No CIS, or network, which shall be used for the processing, storage, or transmission of NATO information, or data, shall be operated without the prior accreditation or approval of the appropriate CIS Security Authority.

1-40. National CIS not connected to a NATO CIS but which process NCI, are to be accredited by the appropriate National Security Authority (NSA). Where national CIS are to be connected to a NATO CIS, the prior approval of the ACO Security Accreditation Authority (SAA) shall be obtained.

1-41. All CIS, media and ancillary devices are to be protected in accordance with their security classification and to a standard at least equal to that afforded to an equivalent "paper" document.

1-42. All CIS-related incidents are to be reported to the relevant CIS Authority by the fastest appropriate means.

This page is intentionally left blank.

CHAPTER 2 – SECURITY ORGANISATION, RESPONSIBILITIES AND PLANNING

2-1. **Role of the Military Committee.** The NATO Military Committee (MC) is responsible for the overall conduct of military affairs and is consequently responsible for all security matters within the NATO military structure. The MC examines all ACO security inspection reports and is informed of all serious security breaches so that the nations may audit the environment to which they are entrusting their classified information.

2-2. **Security Authority.** SACEUR is responsible for the establishment, maintenance and security of all installations and is responsible for Counter Intelligence and Security throughout ACO. SACEUR is accountable to the MC for all security matters within ACO. This includes responsibility for ensuring that a security organisation is set up, that security programmes are devised and executed in accordance with NATO security policy and that the security arrangements are inspected periodically at each command level. SACEUR is also the Security Risk Owner (SRO) for all matters pertinent to ACO, including I&IS with NNEs.

2-3. **Delegation of Security Authority.** SACEUR delegates his[1] security authority to a member of the SHAPE Command Group (CG) not below the appointment of Chief of Staff (COS), called the Delegated Authority (DA), to manage the security risk within ACO related to I&IS with NNEs. Routine matters affecting ACO are handled by the SHAPE Deputy Chief of Staff (DCOS) Strategic Employment (SEM), supported by the senior Intelligence Officer, SHAPE Assistant Chief of Staff (ACOS) J2, as ACO and SACEUR's Principal Security Advisor (ACO PSyA). The ACO PSyA retains the ability to report directly to the DA, when necessary, on highly sensitive counter-intelligence and security matters; details of incident types are contained within AD 065-003, Counter-Intelligence Policy in ACO.

2-4. **Command Responsibility.** Each ACO commander is responsible, through the chain of command, to SACEUR for security throughout his command. Commanders shall prepare local security orders to implement the requirements of this directive. The minimum standards laid down by the nations and incorporated in this directive shall be complied with. Each ACO commander shall set up a security organisation, which is appropriate to the requirements of his command and to the requirements of the ACO Security Authority.

2-5. **Security Appointments.** Each ACO commander shall appoint an officer to exercise staff responsibility for security for the entire area of his command. This officer shall be the ACOS J2, where established, or a staff equivalent. This appointment fulfils the requirement for the commander's senior security advisor and shall be considered as the HQ [title] Principle Security Advisor (HQ PSyA). Roles and resources will dictate who will implement security functions but the overriding requirement shall be to have a structure which is well coordinated and supervised through ownership at CG level. The essential factors are not determined by who does what, but that all critical security functions are undertaken and coordinated. Whenever possible the command staff and theatre security functions should be separate from the HQ Security support area, though it is recognised this may not be possible at every level of command. Typical appointments should include:

[1] When describing commanders as 'he' or using 'his' throughout the document it is understood that this is to be interpreted as 'he/she' or 'his/hers'.

a. At Staff/Force Level

(1) Command Security Advisor (CSyA). The staff security officer shall be appointed the CSyA and have the lead on command-level security policy, inspections, CIS security accreditation within the strict and formal limits of relevant ACO accreditation strategies, security advice on threat countermeasures, security aspects in support of FP and general security coordination. In operational theatres, the senior security staff officer may be known as the Theatre Security Officer (TSO) but shall provide the same standard of security advice expected from a CSyA.

(2) Other Appointments. Depending on the size and role of the command, there should be specific or merged appointments with control and oversight of COSMIC/ATOMAL, COMSEC, and CRYPTO material. Commanders should also ensure that CIS Security Staffs are appointed and closely integrated or coordinated with Command Security Staff.

b. At HQ[2]/Support Element Level

(1) Headquarters Security Officer (HQSO). An HQSO of at least OF-3 level from a NATO member nation, who shall be responsible to his commander for the implementation of ACO security policy and the management of functional security measures. This appointment should be either integrated or closely coordinated with the Provost Marshal in relation to guarding responsibilities.

(2) Directorate or Divisional Security Officer (DSO). The commander shall ensure that his security organisation is appropriate to the size and role of his organisation. Directorate or Divisional chiefs shall appoint a DSO who is charged with the implementation of security policy within the division or staff element. The DSO will receive direction and assistance from the HQSO and CACO.

(3) Document Control Officer (DCO). A DCO shall be appointed who is responsible for the administrative processing of all NATO classified material and the control and accountability of all NATO SECRET documents within the division or staff element.

(4) COSMIC/ATOMAL Control Officer (CACO). If necessary, a CACO shall be appointed. The CACO should be a commissioned officer or civilian of equivalent status and shall be responsible for the control and accountability of all COSMIC and ATOMAL material (NATO SECRET ATOMAL, CTS/A and CTS/B) in accordance with this directive.

(5) COSMIC Control Officer (CCO). Heads of ACO CTS/A Central Registry and ACO component CTS/A Sub-Registries shall be appointed in writing by relevant Security Authorities as CCOs.

[2] 'HQ' may apply equally to 'Installation' or 'Establishment' (AAP-06 refers); however, consideration shall be provided to appointing an Installation Security Officer (ISO) for those NATO establishments where both an ISO and HQSO are required due to the breadth and depth of security requirements.

(6) COMSEC Officer. A COMSEC Officer, if appropriate, shall be appointed to advise in all matters relating to crypto security and to supervise the internal security of the crypto centre. Commander, ACO COMSEC is responsible for organising and directing the COMSEC programme within ACO and will publish regulations pertinent to his area of authority.

(7) CRYPTO Custodian. A CRYPTO Custodian and at least one alternate shall be appointed for each unit holding NATO crypto material. The Custodian shall be responsible to the commander for the receipt, distribution, custody, safeguarding and destruction of all classified CRYPTO material.

(8) CIS Security Officers. Appropriate CIS Security Officers shall be appointed and coordinated with the overall security function.

(9) Security Committee. A Security Committee shall be constituted to include the HQSO, CACO, COMSEC Officer, CIS Security Officer and DSOs. The Security Committee shall meet a minimum of once every 6 months, preferably under the chair of the CG officer who has ownership of security standards.

2-6. **Security Plans and Instructions.** Each ACO commander shall ensure that security plans and instructions are prepared to implement the security measures prescribed in this directive. The plan should form the basis of the local supplement to this directive and should include, but not be limited to:

a. Physical Security. All assets within the area of command shall be encompassed, including the protection of personnel, documents, military assets, buildings and their contents. The exact designation and description of the protection afforded to all Security Areas and Sensitive Zones shall be included. The Physical Security Plan will normally be held as a separate annex to the formation security supplement and shall be prepared in accordance with the more detailed guidance in Part II Chapters 1 and 2.

b. Personnel Security. Implementation of the administration of security clearances, passes and access to classified information. The procedures for civilian and local employees and the procedures for reception and escort (if necessary) of visitors shall be included.

c. Security of NCI. Implementation of local document security procedures for receipt, transmission, classification, destruction and musters.

d. CIS Security. The local implementation of CIS Security in accordance with AD 070-005.

e. Security Awareness and Education. An officer, normally the HQSO, shall be appointed to oversee the regular provision of security education and the maintenance of security awareness throughout the organisation. Personnel are to be made aware of the threat to security and also the minimum standards to which they are to adhere.

f. Security Breaches. Procedures for the reporting, investigation and administration of security breaches.

g. Counter Terrorist Measures. A comprehensive set of procedures to protect the installation from such acts as terrorism, sabotage or malicious damage shall be formulated in accordance with HN assessment of risk. The HN assessment should consider the special risks to the constituents of an international formation in addition to the risks inherent in the environment of the HN. Additional requirements and considerations are contained in AD 080-025, Force Protection.

h. Emergency Protection. Plans should cover the protection, removal or destruction of all material and equipment classified NATO CONFIDENTIAL or above during an emergency, to prevent unauthorised access and loss of availability. Plans for instant emergency destruction within ACO HQs shall be based on periodically reviewed threat assessment and shall give highest priority to the most sensitive, and mission- or time-critical information.

2-7. **Individual Responsibility.** Overall security depends on good personnel security. On an individual basis, personnel are responsible for NATO security as follows:

a. The protection of NCI is the responsibility of each individual who has custody, processes or has knowledge of such information.

b. The application of the minimum standards contained in this directive is mandatory for all personnel.

c. NCI may only be imparted to persons who have the required security clearance and need to know the information in order to carry out their duties. Conversation and the display of NCI is prohibited in the presence of any uncleared person whether or not that conversation takes place in a Security Area.

d. The retention of private records, diaries or papers concerning matters which are or should be classified in accordance with this directive, is forbidden.

e. The unauthorised removal of NATO classified material from official premises is forbidden.

f. Individuals shall immediately report to their Security Officer any incident which might indicate attempted espionage, subversion, terrorism or sabotage, or any unauthorised disclosure of NCI.

2-8. **Internal Security Reviews.** The various formal security inspections outlined in this directive are based on a sampling check. A system of internal reviews, in accordance with the needs of their organisation, shall be implemented by commanders to supplement and complement the formal inspection. HQSOs shall be tasked to complete a rolling review of security arrangements within staff divisions or departments within their Area of Responsibility (AOR) to ensure standards are maintained and to impart best practice across their AOR.

2-9. **Counter-Intelligence Support** to ACO will be provided by ACCI in accordance with the procedures outlined in AD 065-003. Further clarification can be sought through the SHAPE SEM J2X Counter Intelligence and Human Intelligence (CHI) section.

PART II

PHYSICAL SECURITY

CHAPTER 1: Physical Security for Generic Protection and to Counter Espionage and Subversion

CHAPTER 2: Protective Measures against Terrorist and Sabotage Threats within NATO Countries

CHAPTER 3: Protective Measures against Terrorist and Sabotage Threats outside NATO Countries

AD 070-001

FOREWARD TO PART II

Physical Security represents only one aspect of protective security and shall be supported by sound personnel security, security of information, and CIS security measures. The sensible application of all of these measures will give a balanced and cost-effective defence-in-depth to protect NATO assets within the ACO component headquarters that denies surreptitious or forced entry, and deters and detects adversarial activity. PART II of this directive concerns mainly the application of physical measures to counter threats from espionage, subversion, sabotage and terrorism. Security assets such as fences and other barriers will serve to protect against a range of threats and good security planning and organisation should integrate these facilities for both maximum protection and efficiency. Chapter 1 deals with baseline physical security measures and their application to countering the threat from espionage and subversion. Chapter 2 concerns protection from terrorist and sabotage attack within NATO countries while Chapter 3 concentrates on terrorist and sabotage protection outside NATO countries.

CHAPTER 1 – PHYSICAL SECURITY FOR GENERIC PROTECTION AND TO COUNTER ESPIONAGE AND SUBVERSION

1-1. **General Principles.** Within the context of this chapter, the principal objective of physical security is to prevent unauthorised access to NCI. The measures adopted while planning physical security within the ACO component headquarters must be capable of providing protection in two ways: firstly, there is the need to protect such information in the event of forced or surreptitious entry; secondly, there is the need to protect such information from subverted personnel who have legitimate access. The latter “insider” threat is the more difficult to combat and requires internal separation of information and access to classified information governed strictly in accordance with the "need-to-know" principle. Physical security of the ACO component headquarters shall be built upon a system of “defence-in-depth”, using a combination of complementary physical measures coordinated with personnel, document and CIS security measures. Efficiency of the system and cost effectiveness is best achieved by defining physical security requirements, based on threat assessment and risk management, as part of the planning and design of ACO component facilities.

1-2. **Security Requirements.** The premises in which NCI is kept within ACO components will vary greatly, ranging from large command headquarters through to field deployments. Physical security measures employed will therefore be site specific; however, in deciding what degree of physical protection is necessary, account must be taken of a number of factors which will include, but are not be limited to:

a. The level of classification and category of information.

b. The amount of information held (hard copies, computer media storage).

c. The security clearance and need-to-know (NTK) of the staff.

d. The locally assessed threat from hostile intelligence services, and terrorist and criminal activities.

e. How the classified information will be stored.

1-3. **Security Areas.** The cornerstone in the application of physical security is that information classified NATO CONFIDENTIAL (NC) or higher must be handled and stored in a Security Area. Such areas must be clearly identified at points of entry and organised/structured so as to correspond to one of the following:

a. Class I Security Area. An area where NC information or higher and of any category is handled and stored in such a way that entry into the area constitutes, for all practical purposes, access to classified information (e.g. operations rooms, communications centres and classified document registries). Such an area requires:

(1) A clearly defined and protected perimeter through which all entry and exit is controlled.

(2) A control of entry system which admits only those appropriately cleared and specially authorised to enter the area.

(3) Specification of the level of classification and the category of the information normally held in the area, i.e. the information to which entry gives access.

(4) A clear indication that entrance into such areas requires specific authorisation by the local security authority.

b. Class II Security Area. An area where NC information or higher of any category is handled and stored in such a way that it can be protected by controls established internally from access by unauthorised persons, e.g. premises containing offices in which information classified NC and higher is regularly handled and stored. Such an area requires:

(1) A clearly defined and protected perimeter through which all entry and exit is controlled.

(2) A control of entry system which admits unescorted access only to those individuals who are security cleared and specially authorised to enter the area.

(3) To prevent unauthorised access to NCI and uncontrolled entry to areas subject to technical security inspections, provision shall be made for escorts or equivalent controls for all individuals that do not meet the requirements of b (2) above.

Regular maintenance of security systems is necessary to ensure that equipment operates at optimum performance. It is also necessary to periodically re-evaluate the effectiveness of individual security measures and the complete security system. This is particularly important where there is a change in the use of the site or elements of the security system. This can be achieved by exercising incident response plans.

1-4. **Security Area Concept.** The aim of the Security Area concept is to produce a system of physical barriers and access controls to deter, deny or detect unauthorised access to NCI. At its simplest, the system could comprise a dedicated security container controlled in such a way as to prevent such access. In the majority of cases, the system will encompass multiple security layers within a larger controlled area. In all cases the system of controls and physical measures must be carefully designed in order to achieve the aim.

1-5. **Assessment of Requirements.** In deciding what level of physical security is appropriate, it is fundamental that the degree of protection should correspond with the security importance of the information to be protected. The precise combination of measures should be tailored to meet local requirements, provided that the minimum standards laid down in the following paragraphs are met. In all cases, it is important to complement physical security measures with access control and guard force deployment as physical measures have limited value when used in isolation. More detailed advice on the minimum physical measures to be applied is contained at Annex A.

1-6. **Administrative Zones.** Administrative Zones shall be established around or leading up to Class I or Class II Security Areas and requires less stringent security measures. Administrative Zones require a visibly defined perimeter within which the possibility exists for control of individuals and vehicles. The maximum level of

classification that is permitted to be handled, stored or discussed in Administrative Zones is NATO RESTRICTED (NR).

1-7. **Control of Entry.** Control of entry may be exercised over a site, a building or buildings on a site, or to areas or rooms within a building. Control may be electronic, electro-mechanical, by a guard or receptionist, or a physical barrier. The system must be designed to prevent unauthorised access to NCI, but be flexible enough to meet operational requirements. A pass or personal recognition system shall be used to control entry into Class I or Class II Security Areas.

1-8. **Permanent Staff.** For unescorted access to ACO Class I and Class II Security Areas and subject to the provisions of Para. 1-6 above, all permanent staff must be security cleared to NATO SECRET (NS), or higher if appropriate.

1-9. **Visitor Control.** When granting visitor access to a Security Area, a visitor's nationality, security clearance, NTK and any other special access requirements should be considered to determine whether or not the individual shall be permitted escorted or unescorted access. The following criteria must be met:

a. Visitors with the appropriate security clearance may be given temporary unescorted access.

b. Visitors without sufficient security clearance should not be given access to Security Areas as a matter of routine. Exceptionally, escorted access may be permitted, but only when stringent precautions have been taken to prevent unauthorised access to NATO classified material.

c. Contractor personnel (including maintenance and cleaning staff) must either be cleared to the appropriate level or escorted at all times. The clearance level must equate to the level of information to which they may have inadvertent access. Automated Data Processing (ADP) technicians should be cleared to the highest level being processed on the system.

1-10. **Physical Access to NATO Classified Security Areas by Individuals from NNEs.** Individuals from NNEs who, because of their assignment and official duties, need regular interface with NATO staffs may be granted physical access to Class I and/or Class II Security Areas on the condition that the security provisions and security measures detailed in AC/35-D/1040, "Supporting Document on Information and Intelligence Sharing with Non-NATO Entities" are met. Detailed guidance on the application of security provisions within ACO is contained in the Bi-SC Handbook on I&IS with NNEs.

1-11. **Automated Control of Entry Systems.** Pass systems which allow entrance to a Class I or Class II Security Area may be supported by automated identification, which should be regarded as a supplement to, but not a total replacement for, guards. Such access may be remotely controlled from a guard position by a trained and qualified guard provided that:

a. The automatic access door or gate must physically deny access; half barriers are not acceptable.

b. The guard has Closed Circuit Television (CCTV) surveillance over the access area and has some form of voice communication link.

c. The guard has the ability to override the automated access system to deny access.

d. A pass system supplemented with a unique Personal Identification Number (PIN) is highly recommended.

1-12. **Entry and Exit Searches.** Random searches shall be regularly conducted both on entry and on exit from Security Areas. Such searches are intended to deter unauthorised removal of classified information and the introduction of prohibited items. Entry and exit searches should be made a condition of entry to a site or building. A warning notice shall be displayed to indicate that entry and exit searches shall be randomly undertaken.

1-13. **Security Passes.** A positive identification and entry control system is required to achieve compartmentalisation, preclude unauthorised entry and facilitate entry at control points to Security Areas. This can be done by personal recognition, but is more effectively achieved using a security pass system. Records of security passes issued shall be maintained. Passes shall be:

a. Serially numbered.

b. Include identifying particulars of the holder and photograph. There is no requirement for the holder's signature.

c. Unique to the organisation but without identifying that organisation.

d. Show in coded form the areas or type of access which is permitted.

e. Must be visible at all times within Security Areas and removed from sight outside Security Areas.

f. Passes shall not normally be used as identification cards. The only exception to this rule is those types of high-tech security cards with encrypted chips embedded within the card itself.

g. In operational theatres, security passes issued to personnel who do not hold a valid NATO PSC (e.g. locally employed civilians), shall not be removed from the installation. Such security passes shall be highly distinctive from those security passes issued to personnel holding valid NATO PSCs.

h. Reciprocal arrangements may be organised to cater for frequent exchange of visits. These arrangements should include pass exchange at the control of entry point to the Security Area. A common pass system is permissible for co-located headquarters. Pass systems shall be kept under review to ensure system integrity.

1-14. **Security Guards.** Security guards are required to ensure the integrity of Security Areas and NCI. They must be appropriately cleared, trained and supervised as follows:

a. A guard force will carry out duties ranging from control of entry, manning fixed guard posts, carrying out patrols and security checks, manning alarm stations and responding to incidents. They shall be given initial and continuation training to ensure that they are familiar with all aspects of their duties.

b. Proper supervision is important and, as a minimum, will include inspection and briefing at shift change and personal checks by a supervisor at irregular intervals. Detailed written orders are also to be provided.

c. When guards are used to ensure the integrity of Security Areas where they might have unauthorised access to classified information, they shall be cleared to the level of the information to which they may have access.

d. Where arming is considered appropriate, it is essential that host nation authority is obtained and that any specific requirements are complied with. Guards must be properly trained and be given precise instructions on the conditions of use.

1-15. **Security Guard Patrols and Checks.** Patrols and checks of Class I and Class II Security Areas shall take place outside normal working hours to protect NATO assets against compromise, damage or loss. Areas which are not occupied by personnel on a 24-hour basis shall be inspected immediately after normal working hours to ensure that NCI is properly secured. The frequency of subsequent patrols shall be determined by local circumstances (consideration of level of risk, classification of content, other security systems/equipment in place) but, as a guide, should be conducted once every 6 hours.

a. During the initial check, every security container outside strong rooms, vaults or other specified Class I areas shall be checked as soon as possible after working hours.

b. Thereafter, such containers shall be checked periodically at irregular intervals during non-working hours and days.

c. A guard check of strong rooms, vaults or other alarmed Class I areas consists of a physical examination of doors or other openings and of alarm systems to detect signs of intrusion or tampering with security systems.

1-16. **Guard Response Forces.** Each ACO formation shall have a Guard Response Force which shall provide a minimum of two guards to any point of a security incident on the site without weakening the site protection elsewhere. Guard response to alarms or emergency signals shall be tested regularly to ensure that response times are appropriate to local conditions.

1-17. **Intrusion Detection Systems.** An Intrusion Detection System (IDS) may be used to improve security or as a substitute for guards/patrols (but not for response forces) particularly where the guard force does not have direct entry to a Security Area. Careful planning is necessary to ensure that IDS are effective and the notes at Annex A provide HQSOs with more detailed specifications. Where IDS are used as substitutes for patrols, they shall have the following features:

a. They shall provide continuous coverage of the area being protected.

b. They shall be monitored from a permanently manned control point.

c. They shall be permanently connected to a secure standby power supply.

d. The control unit shall be physically protected and the system shall be capable of warning against tampering or malfunction.

e. Perimeter IDS (PIDS) should be used on perimeters to enhance the level of security offered by a fence. As PIDS are prone to false alarms, they should normally only be used with an alarm verification system such as CCTV.

1-18. **Minimum Standards for Storage of NCI.** The following are the minimum standards for storage of NCI in ACO:

a. COSMIC TOP SECRET (CTS) and all ATOMAL. In a strong room, vault or a Class A container with a built-in Group A standard combination lock within a Class I or Class II Security Area with one of the following supplementary controls:

(1) Continuous protection by a cleared guard or duty personnel;

(2) Inspection of the security container not less than every 2 hours, at randomly timed intervals, by cleared guard or duty personnel; or

(3) An approved IDS in combination with a response capability that following alarm activation will result in arrival at the location by guard personnel within the estimated timeframe required to remove or force entry into the security container, or overcome physical security measures in place.

b. NS or NC. Information classified NS or NC shall be secured within a strong room, vault or security container with a Group A or B lock, or equivalent locking device, within a Class I or Class II Security Area.

c. NR. At minimum, information classified NR shall be secured behind a Group C lock, such as a lockable cabinet or office furniture that is located within a Class I and Class II Security Area, or in an Administrative Zone. Particular care shall be taken when NR is handled in Administrative Zones to prevent unauthorised access and eliminate the possibility of overlooking.

Annex B provides additional details on storage criteria.

1-19. **Security Containers.** Security containers used for storing NCI represent the last line of defence of a system of security. Their time delay capability is ascertained by comprehensive tests in order to determine their resistance to undetected access and to those forms of attack to which they are reasonably likely to be subjected. Containers used for the storage of NCI are tested and certified by NATO member nations as follows:

a. Class A. Containers nationally approved for storage of CTS information within a Class I or Class II Security Area.

b. Class B. Containers nationally approved for storage of NS or NC information within a Class I or Class II Security Area.

c. Class C. Office furniture suitable for storage of information classified NR.

1-20. **Vaults and Strong Rooms.** Vaults or strong rooms shall be constructed to the standards specified by the host nation for the protection of the NCI involved. A vault or strong room will be required for the open storage or permanent display of NC or above in areas that are not permanently manned. Note that a vault need not necessarily be a Class I Security Area and vice-versa. However, where a vault is also a Class I Security Area, appropriate measures must be taken to observe the NTK principle.

1-21. **Locks.** Locks used with security containers and rooms in which NCI is stored are also tested and certified by nations into Group A, B and C categories for use with the corresponding category of container. Detailed specifications for locks are at Annex B.

1-22. **Combination Settings.** Combination security locks are much more secure than key operated locks because they are more resistant to tampering and because the combination itself is much less vulnerable than a key. Conversely, the compromise of a security combination is likely to cause extensive damage as it might permit surreptitious and undetected access to NCI for long periods. Combination settings shall be given the same level of security protection as the classified material that they protect. Annex B provides detailed requirements.

1-23. **Security Keys.** Security keys are those, which operate locks fitted to provide protection to classified material. Therefore, it follows that security keys are those for access to:

a. Security containers.

b. Secure conference rooms.

c. Technically Secure Areas (TSAs).

d. Security briefcases or pouches.

e. Class I or Class II Security Areas.

f. This list is not comprehensive and the keys to exterior gates and external doors, telephone frame rooms, junction boxes, and similar unclassified but important facilities shall also be controlled. Specific rules for the control of security keys are included at Annex B.

1-24. **Office Security.** Each ACO component shall make arrangements to ensure the security of NATO classified material in individual offices. The practice to be followed may vary according to local circumstances but the following minimum standards shall be applied:

a. Overlooking. Appropriate measures must be taken to protect NCI from the risk of overlooking.

b. Unattended Offices and Desks. During normal working hours, personnel may leave NS and below information out in unattended offices within Security Areas subject to the following precautions:

(1) The office room shall be secured with a lock approved by the HQSO.

(2) Classified documents shall be protected against overlooking.

(3) Windows shall be secured.

(4) The security keys to the doors shall be safeguarded.

(5) The maximum unattended period shall be specified in the ACO component Security Supplement to this Directive.

c. Clear Desk Policy. At cease work, the surfaces of desks and other office furniture shall be cleared of all papers to facilitate security checks.

d. Security Checks. A system shall be established to ensure that:

(1) Personnel having custody of NATO classified material have properly secured it in an approved security container at the close of the working day;

(2) That a second person has carried out an independent check;

(3) That every Security Area within each ACO compound housing material classified NC and above is periodically checked by security guards outside of duty hours.

(4) ACO Form 77, “Classified Container Check Sheet” should be used for this purpose.

1-25. **Eavesdropping.** Offices or areas in which sensitive NCI is regularly discussed shall be protected against active and passive eavesdropping (audio and video surveillance) attacks where the risk warrants it. Protection against passive eavesdropping, such as the leakage via insecure communications, direct overhearing or direct observation, may involve soundproofing of designated areas, seeking technical advice and protection against active eavesdropping; for example leakage via implanted devices will require a technical and physical security inspection of the area and its furnishings and equipment by HQ Security Office personnel. Such areas shall be designated as TSAs.

1-26. **Technically Secure Areas.** TSAs shall be established where CTS is regularly discussed. TSAs may also be established in areas where particularly sensitive NS material is regularly discussed and where the risk warrants it. TSAs shall be designated in writing by the ACO component Commander and a certificate of compliance shall be forwarded to the ACO Security Authority. A TSA facility manager shall be appointed, responsible for maintaining the strictest standards of physical, technical and procedural security measures. Annex C provides detailed guidance but the following minimum standards shall be applied to protect against technical attacks and eavesdropping:

a. A full record of the current status of the TSA shall be maintained in the TSA facility profile (Annex D refers).

b. Technical Surveillance Countermeasures (TSCM) inspections shall be carried out annually. This service can be obtained from ACCI by submitting an ACO Form 165, “Counterintelligence Technical Security Request”.

c. TSAs shall be subject to regular physical inspections. These must also be undertaken following any unauthorised entry. A physical inspection by trained security staff shall be carried out following maintenance work; in such cases the HQSO must also consider the need for a technical inspection.

d. Access control into a TSA shall be enforced at all times. Unescorted entry shall be limited to permanent staff (personnel from NATO member nations). Visitors shall be escorted at all times.

e. TSAs shall be kept locked by an approved method when not occupied and keys shall be considered as security keys.

f. No item of furniture shall be brought into TSA until it has been physically examined for eavesdropping devices by trained security staff.

g. No item of electric or electronic equipment shall be brought in until it has been technically inspected and approved by ACCI.

h. Telephones should not normally be installed in TSAs. However, where their installation is unavoidable, they must be provided with a positive disconnect device if the nature of the telephone system makes this acceptable.

i. Mobile communication devices are prohibited from being introduced into TSAs.

The number of TSAs shall, by necessity, be limited. Nevertheless, HQSOs may wish to identify other areas, e.g. Flag Officer's Suites, where it may be appropriate to apply some of the above measures. The availability of technical support in such cases is likely to be limited.

1-27. **Conference Rooms.** Conference and briefing rooms are particularly vulnerable to eavesdropping and must be protected accordingly. Conference rooms, which fulfil the criteria at paragraph 1-26, will be designated as TSAs. All other conference rooms used for the discussion of NC and above must be under continuous control. Furthermore, they shall be secured when not in use, keys and combinations shall be controlled, non-cleared personnel shall be excluded and maintenance and cleaning personnel shall be escorted. Conference rooms should be subject to periodic physical inspections and technical inspections where the risk is high. Essential, non-secure telephones must meet COMSEC requirements. Mobile communication devices are prohibited from being introduced into any conference room where NATO classified subjects are discussed. To provide a visual reminder, signs prohibiting mobile telephones and devices shall be posted at the entrance of all conference rooms. Mobile communication devices shall be turned off and left with security personnel at a reception area for safekeeping.

1-28. **Counter Intelligence Technical Security Programme.** TSCM are the techniques used to prevent, detect and neutralise hostile intelligence efforts to obtain information through the introduction of a monitoring device or the exploitation of weaknesses in TSAs, Conference Rooms and Security Areas. TSCM services are provided by ACCI and comprehensive advice on the scope of the TCSM Programme is outlined within Annex C.

1-29. **Electrical Equipment in Security Areas.** Electrical and electronic equipment represent a variable risk either through exploitation for eavesdropping or from retransmitting or emanating of classified material. In normal circumstances, the risk is low but the following procedures shall be observed:

a. Official Equipment. Electrical equipment introduced into a Class I or Class II Security Area shall be installed in accordance with the regulations contained in AD 070-005, “ACO CIS Security Directive,” which also contains regulations pertaining to official mobile communication devices. ACCI must check equipment on which CTS, ATOMAL or other codeword material requiring special handling may be processed before such processing starts.

b. Private Equipment. Introduction of privately-owned electrical equipment into a Class I or Class II Security Area shall be strictly limited, authorised by the HQSO, and installed in accordance with the regulations contained in AD 070-005, “ACO CIS Security Directive.”

CHAPTER 2 – PROTECTIVE MEASURES AGAINST TERRORIST AND SABOTAGE THREATS WITHIN NATO COUNTRIES

2-1. **Introduction.** The physical security measures described in Chapter 1 of Part II, mainly address the broader threats that physical security can help diminish. Those elements shall always be taken into account in security planning and organisation. This chapter deals with threat within NATO countries and Chapter 3 deals with threats outside NATO countries. This chapter lays down the policy for counter sabotage and counter-terrorist measures within ACO.

2-2. **Threats and Risks.** The risks to NATO civil and military bodies arising from threats to them from sabotage or terrorism may be of six types:

a. The general safety of personnel.

b. The denial of essential supplies and services which will prevent or degrade mission performance.

c. Physical damage.

d. The disruption of the execution of the mission.

e. The disruption of the freedom of movement.

f. The disruption of general security and stability inside the territory of the NATO member states.

2-3. The potential threat against NATO civil or military bodies and individuals assigned to NATO from terrorist activity may arise from:

a. Terrorist organisations (which may include groups and individuals) who might select NATO as a target.

b. Sabotage attacks causing damage to property, incapacity of individuals and/or loss of essential supplies and services.

c. Organised crime.

d. Civil unrest.

2-4. **Types of Threat.** The threat of violence against NATO civil and military bodies may include:

a. Bomb or light weapons attacks, car bombs, carrier bag type bombs, postal bombs and blast incendiary devices.

b. Assassination, abduction, holding as hostages or intimidation of NATO personnel or their families.

c. Demonstrations, which may be organised with violent intent, may lead to violence/damage through confrontation.

d. Direct attacks on and unlawful occupation of NATO premises or property.

e. Hoaxes, particularly false bomb warning, with intent to harass or imbalance security forces in anticipation of an attack elsewhere.

f. Operations against essential/vital CIS, including cyber-attacks on the integrity and/or availability of these systems.

g. Disabling by force of weapons, armoury and hardware essential for achieving the mission.

h. The use of chemical, radiological or biological devices.

2-5. **HN Responsibilities.** HNs are responsible for the external protection of ACO component headquarters within their national territory. HNs are also responsible for keeping the commanders of ACO components informed of the threats from hostile intelligence services and subversive organisations, providing them with general assessment of the terrorist threats and for informing them whenever a specific threat arises. NATO member nations will ensure, unless otherwise agreed, that information concerning threats, pertaining to ACO components and their personnel located outside their respective territories, is passed on bilateral channels from nation to nation.

2-6. HNs will notify ACO components of the specific additional counter-terrorist measures that they should plan and implement under different levels of threat.

2-7. HNs are responsible for providing such security personnel and protective security equipment for the protection of ACO personnel under terrorist threat outside the premises of ACO components as are required in accordance with host country's national protective security standards and procedures. The designation of personnel to be considered under terrorist threat, as well as the security measures to be put into effect for their protection are determined by the security authorities of the HN, after taking into account proposals with justification from interested ACO components.

2-8. In respect of each ACO component on national territory, HNs will nominate points of contact for passing information on threat assessments and for coordinating internal security plans.

2-9. **Parent (or Sending) Nation Responsibilities.** Parent NATO nations will ensure that security considerations are taken into account when selecting residences for their personnel, utilising the expertise of HN security authorities. Expenditure by parent NATO nations on physical security improvements will be confined to residences officially funded by them.

2-10. The deployment of security personnel and the provisions of protective security equipment by parent NATO nations to counter any terrorist threat against their nationals must be coordinated with the HN’s security authorities and the ACO component concerned.

2-11. Parent NATO nations will inform the HN's security authorities and the ACO component concerned of any specific threat existing against any of their nationals on the ACO staff or in national delegations, military representatives or liaison missions collocated with the ACO components.

2-12. **ACO Component Responsibilities.** ACO commanders are responsible for planning internal security measures to protect their installations and personnel. HNs must be consulted to ensure that plans are comprehensive and properly coordinated with external measures. ACO components are responsible for additional planning and implementing counter-terrorist measures for the protection of their installations to include residences provided by NATO/ACO and all personnel located within their premises. Senior ACO personnel should be identified by ACO components to the host and parent nations. ACO commanders are to maintain effective liaison with HN security authorities and the responsible ACCI Regional Office or Detachment. Such liaison should be achieved through nominated points of contact on both sides in order to exchange intelligence and coordinate plans; specific areas to be covered include:

a. Obtaining a general assessment of the terrorist threat.

b. Making arrangements for exchanging information regarding specific threats.

c. Coordinating counter-terrorist measures commensurate with the assessed threat.

2-13. ACO commanders are to maintain formal liaison via NATO/ACO approved channels with ACCI and the security authorities of NATO parent nations of personnel within their formations for coordination of counter-terrorist measures in the event of a special threat existing:

a. Against such personnel from terrorist organisations operating in their parent country, or

b. Against citizens of a particular country.

2-14. ACO commanders are to implement the standard NATO Alert System as described at Annex E and define responsibilities for implementing pre-planned measures to deal with the threat.

2-15. ACO commanders are to institute procedures to report incidents of terrorist activities to host and parent nations, and to SHAPE SEM CCOMC. SHAPE SEM CCOMC will subsequently alert the relevant directorates/personnel within SHAPE, as well as reporting the incident to NATO HQ (SITCEN) for the attention of the NATO Office of Security (NOS).

2-16. **Scope of Security Protection.** Security protection measures must be arranged to guard against the risks of physical damage, denial of essential supplies and services, and death or injury to personnel. Many of the measures in place to protect NATO classified material will also provide defence against sabotage or terrorism, but ACO commanders will have to consider what additional protective measures are required. Some of these physical and procedural measures will need to be permanently in place whereas others can be provided on a contingency basis. In the final analysis, the resource implications required for the protection of an installation and its personnel must be balanced against the operational value of the installation and the risk to personnel; proper planning is the key to an effective security posture.

2-17. **Security Planning - Design of Installations.** The design of ACO component's installations shall take into account security considerations (security by design) and shall

include such material protection and emergency standby equipment as is considered necessary for:

a. Essential operational functions to continue.

b. The preservation of NATO assets (information, material and infrastructure).

c. The general safety of all personnel.

2-18. ACO component commanders shall prepare a detailed Internal Security Plan (ISP) outlining the security measures which will be implemented to protect NATO personnel, their families and NATO assets. The aim of the plan shall be to reduce vulnerability by deterring, detecting, or mitigating the consequences of a terrorist attack and/or act of sabotage. The plan shall also identify options for additional security measures or procedures (for example searching of visitors), which are applied incrementally as the alert states increase and can be removed as the alert states decrease. Additionally, the plan should be drawn up in close consultation with the appropriate HN authorities to ensure coordination of security measures. The plan shall be founded on a statement of requirements that includes:

a. The identity of the vital assets within the installation or establishment.

b. The impact on operations resulting from a loss of those vital assets.

c. A detailed analysis of the installation or establishment's vulnerable points, including an assessment of the likely methods of attack to which they are vulnerable.

d. Examples of elements which should be considered for incorporation in the ISP are detailed within Annex F and at Para 2-19.

2-19. **Internal Security Plan.** The completed ISP shall be signed by the ACO Component Commander and shall include:

a. Threat assessment. Terrorist/sabotage threat assessment shall be provided quarterly or immediately when the threat is identified by a designated team of security subject matter experts in coordination with the HN security authorities.

b. Risk management. This management process shall include, as a minimum, criticality and vulnerability assessments.

c. Security Alert States and associated minimum security measures as detailed at Annex E.

d. The Incident Response Plan shall also contain:

(1) Identification of the authority responsible for ordering the various stages of the plan to be put into effect and of the official responsible for implementing the specific measures listed in the plan.

(2) Designation of responsibilities for exercising command and control (C2).

(3) Contingency arrangements for support and back-up forces.

(4) A description of actions by NATO security forces on and off ACO component premises permitted under the laws of the HN.

(5) Alternate means of communication for security forces.

(6) Specific actions and responsibilities associated with implementation of each Alert State measure.

e. A Consequence Management Plan, which shall include:

(1) Appropriate first responder personnel whose function is to mitigate loss of life/injury to personnel and damage to structures/assets. First responders include, but are not limited to: medical, personnel, fire and rescue teams, Chemical, Biological, Radiological and Nuclear (CBRN) decontamination units and security personnel.

(2) Appropriate planning for both crime scene investigation by law enforcement personnel and personnel casualty/property damage mitigation responses.

2-20. **Training and Inspections.** The ISP shall be implemented as a Commander's Order and practiced at least once a year to ensure its effectiveness. ACO component commanders shall train their staffs (both resident security/emergency personnel and staff across all functional areas) in reacting to different scenarios commensurate with the current threat assessment by formal instruction and by exercises arranged, as appropriate, with the HN. Exercises should include alerting staff outside normal working hours. Validity of the ISP and records of trainings shall be inspected during security inspections. The results and recommendations on corrective actions, if required, shall be included in the security inspection reports.

2-21. **Standard NATO Alert System.** A Standard NATO Alert System exists for all ACO component headquarters. This Alert System consists of 4 graduated alert states: ALPHA, BRAVO, CHARLIE and DELTA. Each alert state attracts basic minimum measures which are applicable throughout ACO. The standard NATO alert system is detailed at Annex E.

2-22. **Receipt of Indications and Warning of Terrorist Activity.** Indications and Warning of terrorist activity against ACO component's assets and personnel will normally be received from the HN's security authorities or from the local police forces. These warnings may also be received directly by an ACO component in the form of a threat or a warning from a terrorist organisation, and finally as an attack on an ACO component asset or personnel.

2-23. **Reporting Threats of Terrorist and Sabotage Activities and Declarations of Alert States.** To avoid duplication of reports and to ensure that the information is complete, threats or an actual act of sabotage or terrorism and resultant declarations of alert states, shall be reported as follows:

a. When information has been received from a HN's security authority, who will specify the level of protection that shall be afforded to the source of information. ACO components shall report to their chains of command the following:

(1) The authority originating the information.

(2) The nature and consequences of the threat or incident.

(3) The action taken.

(4) If the incident requires the NATO Alert State to be raised to BRAVO or above, ACO components shall report the change to their immediate chain of command for reporting to the SHAPE SEM CCOMC (for the attention of ACO Security Authority). Any subsequent reduction in the declared NATO alert state is to be similarly reported.

b. When information originates within an ACO component, the component concerned shall report the specific threat or incident and origin together with the alert state declared if BRAVO or above to HN security authorities and to their immediate chain of command for reporting to the SHAPE SEM CCOMC (for the attention of ACO Security Authority).

2-24. **Budgeting for Physical Protection and Other Protective Material.** ACO components requiring funds for physical security and other protective material are to request funds through SHAPE. The following types of requests are most likely:

a. Physical Protection. Requests for funding of physical protection of their premises (including official residences) are to be supported by a threat assessment produced by the HN's security authorities and by details of the specific aspects of the threat, which would be countered by implementation of the physical security measures.

b. Special Communications Systems. Requests for funding for special communications systems to be used outside NATO installations as part of counter-terrorist and counter-sabotage measures shall require a justification showing full coordination with HN's security authorities.

c. ACO Security Personnel. Personal protective material such as bulletproof clothing and special arms may be acquired from NATO funds in reasonable quantities. It should be noted that only in exceptional cases should funds be approved for acquisition of such material for use other than ACO Security Personnel. When considering such an exceptional purchase, attention must be paid to national caveats and restrictions as applicable.

2-25. **Security Staff.** ACO components are to consider counter-terrorist and counter-sabotage aspects when establishing or reviewing guard arrangements for their headquarters. Personnel for the personal protection of senior ACO officials should be maintained separately from other security forces and their employment must be coordinated between ACO establishments, HN security authorities and/or Parent Nation.

2-26. **Coordination and Monitoring of Counter-Terrorist and Counter-Sabotage Arrangements.** Counter-terrorist and counter-sabotage arrangements and activities related to ACO components shall be coordinated with HN's security authorities, together with ACCI, and will be monitored by NOS. In this regard, ACO components are to forward, to the ACO Security Authority, a copy of any changes to the general threat assessment applicable to them with a copy of the ISP detailing specific measures implemented to

counter the identified threat. The ACO Security Authority will inform NOS of any changes in counter-terrorist posture. Counter-terrorist arrangements will be subject to examination during the security inspections of ACO components.

This page is intentionally left blank.

CHAPTER 3 – PROTECTION MEASURES AGAINST TERRORIST AND SABOTAGE THREATS OUTSIDE NATO COUNTRIES

3-1. **Introduction.** This Section lays down the policy for counter-terrorist and counter-sabotage measures for ACO forces and installations (assets) deployed outside the territory of the NATO member states (non-Article 5) and shall be considered in conjunction with direction and guidance provided in AD 080-025, “ACO Force Protection”. These measures are implemented in areas where ACO personnel and installations (assets) are deployed where insufficient support can be relied upon to provide an adequate response to a terrorist/sabotage threat. Before implementing the requirements of this Chapter, the baseline physical security measures set out in Chapter 1 shall be considered. The counter-terrorist and counter-sabotage measures described in this chapter only apply to NATO-led non-Article 5 operations and where the HN’s security structure, if it exists at all, falls outside the jurisdiction of a NATO nation. The measures set out in this section will become applicable when threats arise that may endanger NATO forces and installations. In such circumstances, protective security measures shall be applied and coordinated to complement and enhance the local FP Plan.

3-2. **Risks.** The risks arising from threats may be of six types:

a. The general safety of personnel.

b. The denial of essential supplies and services which will prevent or degrade mission performance;

c. Physical damage.

d. The disruption of the execution of the mission.

e. The disruption of freedom of movement (FoM).

f. The disruption of general security and stability outside the territory of the member states.

3-3. **Threats.** Threats from organisations, groups and individuals who might target NATO personnel and assets include:

a. Bomb or light weapons attacks, vehicle borne improvised explosive devices (IEDs), carrier bag type bombs, postal bombs and blast incendiary devices.

b. Assassination, abduction, holding as hostages or intimidation of NATO personnel or their families.

c. Civil unrest through demonstrations, which may be organised with violent intent, or in regard of which there are clear indications that they may lead to violence/damage through confrontation.

d. Direct attacks on and unlawful occupation of NATO premises or property in the same way that has occurred with embassies and/or international missions.

e. Hoaxes, particularly false bomb warning, with intent to harass.

f. Information operations against essential/vital CIS, including cyber-attacks on the integrity and/or availability of these systems.

g. CBRN, in particular, chemical and biological attacks.

h. Disabling by force of weapons, armoury and hardware essential for achieving the mission.

3-4. **Assessing the Threat.** The potential threat will be subject to an assessment prior to the adoption of any counter-measures. Although circumstances and conditions may vary per operation, the process of assessment, as a minimum, should ensure that:

a. As far as possible, the sources of threat information are assessed to be reliable.

b. Analysis of threat information justifies implementation of terrorist counter-measures.

c. The threat assessment is timely and current.

d. A local risk management strategy is developed.

3-5. **Responsibilities.** Allocation of security responsibilities and tasks will be governed by the four differing environments in which NATO forces may operate outside the territory of the NATO countries:

a. Permissive, with full support of the HN.

b. Semi-permissive, in which the HN authorities are generally cooperative, but without sufficient means or control to provide effective support.

c. Non-permissive, where local authorities and population are hostile or not supportive.

d. In international waters and/or airspace.

3-6. **Responsibilities of Non-NATO HNs:**

a. In a permissive environment, NATO will aim to reach an arrangement with the HN providing the external protection of NATO civil and military bodies. This arrangement will strive to include the same provisions and support as agreed with HNs inside the NATO AOR as described in the first Part of this document.

b. In a semi-permissive environment, similar arrangements should be established with the HN. However, the HN may require the support of NATO means and capabilities to ensure/enforce provisions/support can be provided as agreed.

c. In a non-permissive environment, no HN support should be expected.

3-7. **Responsibilities of NATO Commanders:**

a. The planning, including threat assessment, decision-making, coordination and implementation, of security measures.

b. Concepts of Operations (CONOPs) that establish a security regime and organisational structure to adapt to threats.

c. Checks, through the NATO Chain of Command, to establish that locally employed personnel do not represent a threat to NATO forces and assets.

d. Security principles, as laid down in Part II of AD 070-001, should be taken into account in the planning process for every Operational Plan (OPLAN).

e. In a permissive or semi-permissive environment, NATO commanders should take full account of the aforementioned agreements with HNs and of the respective responsibilities of HNs and Troop Contributing Nations (TCNs).

f. In a non-permissive environment, HN support will devolve to the NATO commanders. They will, however, ensure that they operate within the mandate as provided within the approved OPLAN.

g. In all circumstances, NATO commanders will ensure that coordination and the exchange of information will take place with all parties involved, e.g. by establishing liaison with the HN, as appropriate and through the Chain of Command with all TCNs and taking into account extant security regulations.

h. NATO commanders may augment, as necessary, the minimum measures, as shown in Alert States. The Strategic Commander may institute procedures to waive Alert State minimum measures, as appropriate.

3-8. **Responsibilities of TCNs**

a. TCNs, along with NATO, remain responsible for the provision of security support to their national forces. This includes security-vetting checks that ensure locally employed personnel do not represent a threat to NATO forces and assets.

b. In a permissive or semi-permissive environment, TCNs are responsible for arranging the exchange of information of a terrorist/sabotage threat/incident through the NATO liaison, as appropriate.

c. NATO forces shall operate using authorised Rules of Engagement (ROE). TCNs may limit the applicability of ROE for execution by its national forces. The NATO commander will be informed of such national restrictions.

3-9. **Reporting of Terrorist or Sabotage Activities.** Reports concerning terrorist/sabotage threats or incidents by the various military or civil authorities shall specify:

a. The authority originating the information.

b. The nature and the consequences of the threat or incident (who, what, why, when, where and how).

c. The action taken.

3-10. To ensure adequate information of appropriate authorities, threats or actual terrorist/sabotage incidents shall be reported as specified below:

a. NATO commanders shall report to the next headquarters in the chain of command and to subordinate commanders.

b. To ensure similar security measures, non-NATO forces in NATO-led operations shall participate in the reporting system in accordance with existing security arrangements.

c. All TCNs will be informed of the specific threat/incident through their national contingent commanders in Theatre, at subsequent levels of command and/or NATO headquarters.

d. As appropriate, HN authorities will inform the NATO commander and/or will be informed of the threat/incident through a designated NATO liaison officer, as agreed in advance with that nation and in accordance with extant security regulations.

3-11. **Internal Security Plan (ISP).** The completed ISP shall include:

a. A terrorist/sabotage threat assessment.

b. A risk management assessment. This assessment shall include, as a minimum, criticality and vulnerability assessments.

c. Security measures, including physical security,

d. An Incident Response Plan which shall contain:

(1) Identification of the authority responsible for ordering the various stages of the plan to be put into effect and of the official responsible for implementing the specific measures listed in the plan.

(2) Designation of responsibilities for exercising command and control.

(3) Contingency arrangements for support and back-up forces.

(4) A description of actions by NATO security forces on and off NATO premises permitted under the laws of the host nation.

(5) Alternate means of communication for security forces.

(6) Specific actions and responsibilities associated with implementation of each Alert State measure.

(7) Use of lethal/non-lethal force together with full details of the ROE to be employed.

e. A Consequence Management Plan, which includes:

(1) Appropriate first responder personnel whose function is to mitigate loss of life/injury to personnel and damage to structures/assets. First responders include, but are not limited to: medical, personnel, fire and rescue teams, CBRN decontamination units, and security personnel.

(2) Appropriate planning for both crime scene investigations by law enforcement personnel, as well as personnel casualty/property damage mitigation responses.

This page is intentionally left blank.

PART III

SECURITY OF INFORMATION

CHAPTER 1: Document Classifications and Markings

CHAPTER 2: The ACO COSMIC TOP SECRET and ATOMAL Registry Systems

CHAPTER 3: Preparation, Transfer, Control and Destruction of Classified Documents

CHAPTER 4: Release of NATO Classified Information to Non-NATO Recipients

This page is intentionally left blank.

CHAPTER 1 – SECURITY CLASSIFICATION AND MARKINGS

1-1. **Introduction.** NATO information falls into three categories: Classified, Unclassified[3] and information Releasable to the Public[4]. All NATO information shall carry a marking indicating its category. This chapter provides direction and guidance relating to the classification and marking of NCI.

1-2. The key objective of marking NCI is to ensure the adequate protection of the information and to support the effective and efficient sharing of information in the conduct of NATO missions, consistent with the appropriate information protection.

1-3. **Information Sharing.** NCI shall be managed with an emphasis on 'responsibility-to-share' balanced by the security principle of NTK, and shall also be managed to facilitate access, optimise information sharing and re-use, and reduce duplication in accordance with security, legal and privacy obligations. Accordingly, when required NATO information should be clearly marked to facilitate information sharing.

1-4. **Information Access and Releasability.** NATO Security Policy (NSP) requires that access to, and release of, NCI is strictly controlled. Accordingly, NCI shall be clearly marked to identify the required level of protection and to indicate access or releasability where appropriate in accordance with Part III Chapter 4 of this Directive.

1-5. **Consistency of Security Markings.** Markings on NCI shall be consistent to enable information sharing, cooperation, and effective and efficient processes.

1-6. **Public Release and Disclosure of NATO Classified Information.** NCI, which from its inception is intended to be communicated to the public as part of NATO's public diplomacy and outreach activities, e.g. a press release shall not carry standard NATO markings. NCI being made available to the public as a result of public disclosure should retain the original markings, with annotations indicating its change of categorisation. This applies equally for NCI released to a specific public entity such as a court, parliamentary commission, or similar.

1-7. **Security Classification.** If it is determined that a security classification is warranted, a conscious decision is to be made by the originator in selecting a level which is consistent with the sensitivity of the information.

1-8. The overall NATO security classification of a document shall be at least as high as that of its most classified component. In addition, the covering document shall be marked with the overall NATO security classification of the information to which it gives access to. When covering documents are used they shall contain a statement clearly identifying their NATO security classification or marking when separated from the attachments and shall be protected accordingly.

---

[3] Within NATO, the marking UNCLASSIFIED, combined with an ownership marking, indicates that the information does not require security protection but is to be used for official purposes. The combined marking constitutes a proprietary marking and carries no security connotation.

[4] NATO UNCLASSIFIED information and information releasable to the Public shall be managed, protected and handled in accordance with the NATO Information Management Policy C-M(2007)00118 and the Management of Non-Classified NATO Information (C-M(2002)60).

1-9. **Component Security Markings.** Where possible, component parts such as paragraphs, enclosures, annexes, etc. of documents classified NR and above should be marked appropriately by the originator to facilitate decisions on further dissemination. The top and bottom of each page of the document shall be marked with the overall NATO security classification of the document.

1-10. Individual annexes, appendices, attachments and enclosures may be marked as per Para. 1-9 above at a level lower than the overall NATO security classification of the document.

1-11. **Aggregation Principle.** When a large amount of NCI is collated together, the original security classification markings shall be retained. The collective information shall be assessed for the impact of its combined loss or compromise upon the organisation. If the overall impact is assessed as being higher than the impact of the actual individual NATO security classifications, then consideration should be given to handling and protecting it at a level commensurate with the assessed impact of its loss or compromise.

Note: Both over-classification and under-classification should be avoided. The dangers of under classification are evident, but over-classification can be equally dangerous in that it debases the security system and adds unnecessarily to the burden of administration. The recipient should bring cases of apparent over-classification or under-classification to the attention of the originator. If the originator decides to reclassify the document, all addressees shall be informed in writing.

1-12. **Authority to Apply CTS Classification.** The number of staff members within ACO component HQs who can apply the CTS classification shall be kept to the minimum level consistent with efficient operations. Each ACO component commander shall designate in writing the names and appointments of those who are granted this authority.

1-13. **Change of Classification.** NATO classified material may be either upgraded, downgraded or declassified only by, and with written consent of the originator. Where the originator cannot be determined, the successor organisation or higher authority shall assume the responsibility of the originator. When NATO classified material includes information from another NATO component or agency, or a national source, written consent of that component, agency or nation is to precede change of its classification.

1-14. When NCI originating from a NATO Nation(s) or NATO Civil or Military body(ies) is collated into a new product, that information shall not be downgraded or declassified without the written consent of the originator.

1-15. The originator is responsible for ensuring that recipients are promptly notified in writing when the NATO security classification level of accountable NCI is changed, or the information is declassified.

1-16. Originators of NCI within ACO shall reassess classification levels of their originated documents at 5-yearly intervals with a view to downgrading, declassifying and eventual public disclosure. In all cases, NCI shall be subject to review for declassification and public disclosure after 30 years (50 years for Intelligence and Nuclear Information).

1-17. **Individual Responsibility.** It is the responsibility of all individuals within ACO components who produce or use NCI to follow the classification, marking and protective measures set out in this Directive.

1-18. **Security Markings Applied to NCI.** The security markings to be applied to NCI are composed of four elements, each of which has a specific purpose:

a. Ownership.

b. Classification.

c. Releasability and/or Dissemination Limitation marking.

d. Administrative and/or Category marking.

1-19. **Ownership Marking.** All NATO information should carry an ownership marking indicating the information domain that governed the creation of the information item, e.g. NATO, NATO/Partners for Peace (NATO/PfP), the latter indicating collective ownership of the information. Dedicated ownership information domain markings are established uniquely for NAC-approved cooperative activities (missions, operations, exercises that generate their own jointly produced information). Cooperative activities where participants essentially exchange/release their own information amongst each other do not require the establishment of a dedicated domain marking.

1-20. In cases when NCI created in the context of one information domain (e.g. NATO/PfP), needs to be communicated beyond the originating community, an appropriate releasability marking shall be applied.

Note: A releasability marking does not transfer the ownership of information.

1-21. **Classification.** Security classifications indicate the sensitivity of NATO information and are applied in order to alert recipients to the need to ensure protection in proportion to the degree of damage that would occur from unauthorised access or disclosure.

1-22. **Revision of Classification.** In order to ascertain whether or not the existing security classification remains valid, within ACO components all accountable NCI shall be subject to periodic review:

a. CTS documents originated within ACO are to be reviewed no less frequently than once every 5 years to ascertain if the CTS classification still applies.

b. NS documents originated within ACO shall be reviewed no less frequently than once every 10 years, with downgrading action taken where considered appropriate.

1-23. Such a review is not necessary in those instances where the originator has predetermined that specific NCI shall be automatically downgraded after a predetermined period and the information has been so marked.

1-24. **Releasability.** In support of information sharing, it may be necessary to release some NATO information beyond the information domain to which it would typically be available, e.g. to a NNE. In this case, the originator, based on relevant ACO component Delegated Authority's decision, shall apply such releasability marking when the document is ready for collaboration and/or publication. The releasability marking shall be clear and complete. Originators shall take both current and anticipated information sharing requirements into consideration when applying the relevant elements of the releasability marking.

1-25. In all instances, releasability is based upon a positive determination by the originator of the 'responsibility-to-share' balanced by the security principle of 'need-to-know'. The releasability marking indicates an extension of accessibility beyond the original information domain. It expresses the intent to share the information further and to enable accessibility and accordingly, it is not, on its own, a distribution instruction. Furthermore, the application of a releasability marking will not entail more restricted handling or increased security protection of the information item carrying the releasability marking.

1-26. In the event that information needs to be shared, after initial publication, with entities beyond the original intent and markings, the procedures for release summarised in this directive and provided by NSP, the Policy on the Management of NATO Non-Classified Information and/or the NATO Policy on Public Disclosure[5] should be followed as appropriate to obtain agreement to the proposed additional information sharing.

1-27. **Dissemination Limitation Markings.** Contrary to releasability markings, dissemination limitation markings may be applied by the originator to indicate that dissemination of the information is limited to only some of the entities that would be implicit in the initial domain marking such administrative or dissemination limitation markings are intended to clearly identify the type of information contained therein and the need for limitations to be placed upon access to this information.

1-28. **Administrative Marking/Category Designator.** There are occasions where information access needs to be reduced due to the sensitivity of the content. This includes information which may not require protection but should nonetheless not be widely distributed or shared, e.g. a personnel or a medical file. In such a case, an approved administrative marking should be applied by the originator.

1-29. **Category Designators** (e.g. ATOMAL, BOHEMIA, CRYPTO) identify categories of information that are subject to special handling and protection requirements beyond those determined by the basic NSP and procedures.

1-30. **Application of NATO Information Markings.** All NATO information, regardless of format, should be marked in the manner most suited to the handling of that information. Guidance on the technical implementation of these markings when handling NATO information within NATO CIS (e.g. electronic labelling) is provided to all ACO personnel by the AD 070-005, "ACO CIS Security Directive," with SHAPE SEM J2X IA acting as the point of contact.

1-31. All NATO information intended for printed form or electronic display shall carry a NATO information marking at the centre top and/or centre bottom of each page. Ownership, classification and administrative/category markings shall be indicated in full capitals, in bold. Releasability/dissemination limitation markings shall be indicated in title case, regular script, centred, below the ownership, classification and administrative/category markings. If the latter markings are applied to both top and bottom, then the releasability/dissemination limitation marking shall be applied only to the top of the page.

1-32. The following are examples of correctly presented markings:

[5] C-M(2008)0116.

a. Basic Marking:

NATO RESTRICTED

b. Marking combined with Administrative/Category Marking:

NATO RESTRICTED – STAFF

c. Marking with Releasability Marking denoting specific countries:

NATO RESTRICTED
Releasable to Japan, Switzerland, Ukraine

d. Marking with Releasability Marking denoting a community of countries:

NATO/PfP RESTRICTED
Releasable to KFOR

e. Marking with Dissemination Limitation

NATO/KFOR RESTRICTED
NATO, Sweden, Ukraine Only

1-33. “Limited” indicates that a specific dissemination and access limitation has been imposed by the originator, e.g. information should by strictly disseminated only to the recipients named on the distribution list of the document. In addition to the overall marking applied to an information item, all NCI items shall contain markings relevant to specific component parts in order to facilitate information sharing and re-use. Such markings should be applied as follows:

a. Annexes. Shall have independent ownership and classification markings, which may be identical or different to their main document; they may also carry specific releasability markings which may extend beyond the releasability of the main document;

b. Appendices. Are part of an annex and shall carry the same markings;

c. Enclosures. Shall retain their original markings;

d. Documents classified NC and above. Shall be marked at paragraph and sub paragraph level; these markings may comprise ownership, classification and releasability indications, either inserted in abbreviated textual form, e.g. “NC Rel KFOR”, or in the standardised form of electronic tags at the start of each paragraph or sub paragraph.

e. Presentations. Shall be marked at slide level; when slides are incorporated into documents, the relevant pages shall be marked in accordance with the markings of the slides. The first slide shall be marked to reflect the overall classification of the presentation and shall reflect the highest classification contained within.

f. Classification of References. References to classified documents should not to be classified unless the reference itself contains or reveals classified information. This can normally be avoided by keeping reference details to a minimum.

g. Emails. Emails shall be classified to reflect the classification of the content and attachments. It is strictly forbidden to transfer emails with classified content or attachments via an unclassified network.

1-34. **Overall Classification.** An aggregated information item, e.g. a document with attachments or a collated information product, shall bear the overall marking of the highest classified individual component part, with suitable indications on the classification upon removal of this part. Originators of aggregated information items are responsible for maintaining the coherence of the markings in order to safeguard the interests of the contributors.

1-35. **Website Markings.** To facilitate information sharing in a networked environment, websites containing only information of a level lower than the highest level for which the host network is approved, shall have their web pages marked at that lower level (e.g. a NSWAN website containing only NR information shall be marked as NR). In a similar manner, websites containing only information with a specific information domain marking (e.g. NATO/PfP) or with a specific releasability marking, may be marked accordingly to facilitate information sharing arrangements for individuals from NNEs that are granted access to the NATO network hosting those sites.

1-36. **Changes or Additions to Security Markings.** Appropriately authorised changes or additions to security markings (e.g. downgrading, follow-on release, public disclosure) that occur after initial publication of an information item shall be indicated by annotations, additional cover sheets, or letters of transmittal that clearly indicate the new marking, or the changed status of the information item. This shall include a reference to the document that authorised the change. This concerns in particular the archive copy of the information item, as well as copies that are made available to a NNE, as a result of changes or additions.

1-37. **Automatic Downgrading/Declassification.** In order to facilitate the reclassification of classified information, originators should indicate when a document can be automatically downgraded or declassified. Such notification shall be applied to the first page of the document. In the case of electronically transmitted messages, the downgrading statement, if appropriate, shall be contained in the body of the message.

1-38. **Approved Security Markings.** The use of NATO security markings is governed by legal, security and policy documents agreed by the NATO Nations. All individuals creating, processing, managing or otherwise using NCI shall adhere to the provisions of these documents. The NATO Security Committee maintains and promulgates a table of equivalences that shall be used to ensure consistent and appropriate handling and protection of classified national information introduced into NATO. When national or NATO external classified information items are enclosed with NCI items, a NATO security marking may be added while the existing markings will be retained.

1-39. NATO approved security markings, together with their meaning and source are summarised in the following paragraphs for ease of reference.

1-40. **Ownership Markings.** A number of ownership markings have been developed which reflect the information domain under which the information was created and promulgated. No other markings may be used in the production of NCI. However, inactive markings, e.g. NATO/SFOR, may be maintained in support of Information Management activities such as downgrading or public disclosure, where the original stakeholders may need to be involved.

Ownership Marking	Definition	Source	Status
COSMIC[6]	NATO information subject to the COSMIC security policy used for TOP SECRET.	NATO Treaty, D.C. 2/7, and C-M(2002)49	Active
NATO[7]	Information generated or received (including information received without a specific ownership marking) in the context of NATO activities and subject to NATO security and information management policy.	NATO Treaty, C-M(2002)49	Active
NATO/EAPC	NATO information generated in the context of EAPC activities.	08.11.1991 Rome Declaration, 30.05.1997 EAPC Basic Document	Active
NATO/GEORGIA	NATO information generated in the context of the NATO-Georgia Commission.	15.09.2008 NATO/GEORGIA Framework Document	Active
NATO/HAWK	NATO information generated in the context of the HAWK Programme.	C-M(59)54	Inactive
NATO/ISAF	NATO information generated in the context of operations of ISAF.	SG(2003)0810	Inactive

[6] The marking COSMIC is to be applied exclusively to all copies of TOP SECRET documents prepared for circulation within NATO. The only exception to this rule will be in the event of an emergency when operational needs require that TOP SECRET documents be distributed to, or originated by, units where no COSMIC registry exists. In such cases the word COSMIC should be omitted, but the documents are to be given the security protection appropriate to COSMIC TOP SECRET material (See Part II Chapter 1). The documents are to be incorporated into the COSMIC system as soon as possible.

[7] The marking NATO is to be applied to all copies of classified documents (except those marked COSMIC TOP SECRET) prepared within NATO. It is also to be applied to UNCLASSIFIED documents originated within ACO. The markings COSMIC and NATO signify that the document must not be passed outside NATO except by the originator, or with the originator's consent.

NATO/KFOR	NATO information generated in the context of operations of KFOR.	C-R(98)30	Active
NATO/PfP	NATO information generated in the context of the PfP Programme.	11.01.1994 PfP Framework Document	Active
NATO/RUSSIA[8]	NATO information generated in the context of the NATO-Russia Council (formerly Permanent Joint Council).	27.05.1997 NATO/Russia Founding Act	Active
NATO/UKRAINE	NATO information generated in the context of the NATO-Ukraine Commission.	09.07.1997 NATO/UKRAINE Charter	Active

1-41. Within NATO systems (document, registers, etc.), the indication PUBLIC (or a suitable code) should replace any ownership marking once an information item has been declassified and released or disclosed to the general public. The system indication PUBLIC confirms that NATO has relinquished dissemination control of the item so identified and the information item itself should be annotated accordingly.

1-42. **Classification Markings.** NATO security classification markings indicate the sensitivity of NCI and are applied in order to alert recipients to the need to ensure protection in proportion to the degree of damage that would occur from unauthorised access or disclosure. NATO security classifications and their significance are:

Classification Marking	Definition
TOP SECRET	Unauthorised access or disclosure of this information would result in exceptionally grave damage to NATO.
SECRET	Unauthorised access or disclosure of this information would result in grave damage to NATO.
CONFIDENTIAL	Unauthorised access or disclosure of this information would be damaging to NATO.
RESTRICTED	Unauthorised access or disclosure of this information would be detrimental to the interests or effectiveness of NATO.

1-43. In the event that NATO information does not require a security classification, the following marking shall be used:

[8] Russia is a Special Relations country; however, relations with Russia have been suspended below the Political Level since the annexation of Crimea in March 2014. SACEUR is the only member of ACO exempt from this suspension.

Classification Marking	Definition
UNCLASSIFIED	Such information may carry an administrative or dissemination limitation marking and shall only be used for official purposes, and only individuals, bodies or organisations that require it for official NATO purposes may have access to it.[9]

1-44. Information which from its inception is intended to be communicated to the public as part of NATO's public diplomacy and outreach activities, e.g. a press release, shall carry no markings of any sort.

1-45. **Releasability and Dissemination Limitation Markings.** In addition to the ownership and classification markings, NATO has developed a number of markings that elaborate upon the accessibility of information. These markings either expand or restrict the accessibility inherent in the ownership and classification markings:

Releasability and Dissemination Limitation Marking	Definition	Source
Releasable to …	Indication that the dissemination and access to NCI may be extended to more NNEs than those that are implicit in the ownership marking. These entities must be identified as part of the marking. Groupings of entities, (e.g. KFOR, PfP) must be defined and agreed for general usage throughout NAC before being applied.	AC/35-D/2002
"...Only"	Indication that the dissemination of and access to NCI is limited to only some of the entities that are implicit in the ownership marking. These entities shall be identified as part of the marking (e.g. "NATO CONFIDENTIAL Releasable to KFOR – NATO Only").	AC/35-D/2002
Limited	Indication that a specific dissemination and access limitation has been imposed by the originator. A corresponding instruction must be available. Onward dissemination shall comply with that instruction (as described in 1-46 below).	C-M(2002)49

1-46. Furthermore, the expression 'CLOSE HOLD' is currently in frequent use to indicate a need for dissemination control. This is an unofficial marking used to indicate a temporal sensitivity to information that should not be passed beyond the original addressees.

[9] C-M(2002)60.

Instead of this unofficial legacy marking, NATO policy encourages, depending on intent and content, the use of the marking ‘LIMITED’ or of the marking ‘MANAGEMENT’ for this purpose.

1-47. **Administrative Markings and Category Designators:** Information accessibility and usage may be further delineated by a number of administrative markings and/or category designators that are typically used to indicate handling requirements beyond those indicated by the ownership and classification markings:

Category Designators and Administrative Markings	Definition	Source(s)
ATOMAL[10]	Information concerning nuclear matters and subject to the agreement on the exchange of ATOMIC information, and requiring special handling.	C-M(64)39 C-M(68)41 C-M(2002)49
SIOP	Designator signifying that the information shall be protected in accordance with Special Procedures for Handling of United States Single Integrated Operational Plan Information within NATO.	C-M(71)27
BOHEMIA[11]	Information concerning SIGINT related operations, sources and methods, and requiring special handling.	C-M(2002)49 MC 0101
COMMERCIAL	Information containing commercial proprietary information, e.g. received in procurement actions.	C-M(2002)60
CRYPTO	An identifier for COMSEC keying material or related documentation that is used to protect or authenticate NATO telecommunications and requires special handling.	C-M(2002)49
MANAGEMENT	Information concerning advice on policy and planning affecting the interests of NATO.	C-M(2002)60
MEDICAL	Information concerning medical reports and related material on personnel and units.	C-M(2002)60
PERSONAL	Information to be seen only by the individual to whom it is addressed.	C-M(2002)60

[10] The ATOMAL marking will be applied to nuclear weapons information that has been provided to NATO organisations either by the US (from their "Formerly Restricted Data") or by the UK (from their "UK ATOMIC Information").
[11] All information marked BOHEMIA shall be handled and protected in strict accordance with MC 0101 and its companion AJP.

STAFF	Information containing references to named or identifiable staff.	C-M(2002)60

1-48. **Definition of Terms.** For clarity, a number of terms used within this Chapter are defined below:

a. Access

The right, opportunity and means of finding, using, or retrieving of NCI.

b. Availability

The property of information and material being accessible and usable upon demand by an authorised individual or entity.

c. Confidentiality

The property that information is not accessed by, or disclosed to, unauthorised individuals (without appropriate PSC and/or need-to-know), entities or processes.

d. Information

Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audio-visual forms.

e. Information Domain

The domain where information is created, transformed and shared; where intent is conveyed and where consultation, command and control takes place.

f. Information Management

Information Management is a discipline that directs and supports the handling of information throughout its life-cycle ensuring it becomes the right information in the right form and of adequate quality to satisfy the demands of an organisation.

g. Information Owner

The nation or organisation which creates and maintains content, defines access rules, negotiates and agrees to release constraints, establishes disposition instructions, and is the authority for the life-cycle of information.

h. 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.

i. Originator

The nation or international organisation under whose authority the information has been produced or introduced into NATO.

j. Responsibility-to-Share

The individual and collective obligation to make information available, discoverable and accessible for those entities that require the information to perform their official tasks and services.

CHAPTER 2 – THE ACO COSMIC TOP SECRET AND ATOMAL REGISTRY SYSTEMS

2-1. **General.** This chapter deals with the need to establish both CTS and ATOMAL Registry Systems within ACO for the correct storage, handling, dissemination, receipt and destruction of CTS and ATOMAL information. The direction within this chapter implements within ACO the Agreement between the Parties to the North Atlantic Treaty for Co-operation Regarding ATOMAL Information (hereafter called the Agreement), signed in Paris on 18th June 1964 (Reference C-M(68)41(8th revise)):

a. ATOMAL information is either US Atomic information (Restricted DATA or Formerly Restricted DATA) released under NATO ATOMAL markings which is provided by the Government of the United States of America to other NATO component under the Agreement; or “UK ATOMIC information” which is provided by the Government of the United Kingdom to other NATO components under the Agreement.

b. Special Limitations may be prescribed by the Government of the United States of America on oral, visual, electronic, or printed communications containing ATOMAL information, normally used in nuclear planning activities (see Annex G). Such limitations will be indicated by means of appropriate markings on the face of documents or images. When information transmitted by the United States of America under Special Limitations is contained in reproduced or generated documents or is disseminated by oral, electronic, or visual means, it shall be handled in accordance with the same Special Limitations. Requests for waivers to the restrictions on the dissemination of ATOMAL information under Special Limitations may be submitted to the Government of the United States of America only by the ACO Security Authority.

c. The United Kingdom Government may also prescribe Special Limitations on oral, visual, electronic, or printed communications containing UK Atomic information. Such limitations will be indicated by means of appropriate markings on the face of the documents or images. When information transmitted by the United Kingdom under Special Limitations is contained in reproduced or generated documents or is disseminated by oral, electronic, or visual means, it shall be handled in accordance with the same Special Limitations. Request for waivers to the restrictions on the dissemination of UK Atomic information under Special Limitations may be submitted to the United Kingdom Government only by the ACO Security Authority.

d. References mentioned below in paragraphs (1) to (4) contain policy for the protection of classified information, establishes procedures for the control and handling of CTS and ATOMAL material, and controlling CTS and ATOMAL information. This directive provides supplementary instructions for applying the provisions of these References within ACO. The reference mentioned in paragraph (5) standardises the operating procedures for the ACO CTS/A Registry System. The References provide specifics on matters not covered by this directive:

(1) C-M(2002)49, Security Within the North Atlantic Treaty Organisation.

(2) C-M(64)39, Agreement between the Parties of the North Atlantic Treaty for Cooperation Regarding Atomic Information.

(3) C-M(68)41(8th Revised), Administrative Arrangements to Implement the Agreement between the Parties to the North Atlantic Treaty for Cooperation Regarding ATOMAL Information.

(4) C-M(2007)0118, NATO Information Management Policy.

(5) ACO MANUAL 070-001-003.

e. SHAPE is responsible for preparing and introducing the ACO Manual (AM) 070-001-003 containing all required regulations and standard operating procedures necessary for proper processing of CTS and ATOMAL information within ACO CTS/A Registry System. The offices responsible for the management of information within the respective ACO components are responsible for the formulation, in conjunction with SHAPE SEM J2X, of the respective Supplement to the Manual. This part of the Directive has the following objectives:

(1) To secure and facilitate the distribution and use of CTS and ATOMAL information within ACO under requisite security safeguards;

(2) To provide guidance to ACO personnel on the classification of information concerning nuclear weapons;

(3) To set forth procedures, functions and responsibilities of ACO components for handling and protecting CTS and ATOMAL information.

2-2. ACO COSMIC TOP SECRET and ATOMAL Registry Systems

a. Under the authority of the NAC, each component of the NATO organisation is required to set up a registry system to control CTS and ATOMAL material. This has been established within ACO and is known as the “ACO COSMIC TOP SECRET and ATOMAL (CTS/A) Registry Systems”, designated to perform dual, but separate, functions, controlling ATOMAL as well as CTS classified documents and material.

b. The ACO CTS/A Registry System comprises an ACO CTS/A Central Registry and Control Points (CPs) located in SHAPE and CTS/A Sub-Registries and CPs located in all the international commands and agencies subordinate to SACEUR.

c. The ACO component’s CTS/A Sub-Registries or CPs can be physically located with the headquarters’ Registry; however, they shall be distinct and separate and shall be managed accordingly.

d. The ACO CTS/A Registry System is supervised by the ACO CACO, designated by the ACO Security Authority from among SHAPE SEM J2X SPO staff.

e. The ACO CTS/A Central Registry, ACO component Sub-Registries and CPs shall be supervised by HQ CACOs and their deputies, designated by ACO component Security Authorities from among divisions, directorates or departments responsible for information management. However, Registry CCOs assigned to ACO CTS/A Central Registry, ACO component CTS/A Sub-Registries and CPs shall not be appointed as HQ CACOs or Deputy HQ CACOs, to avoid conducting

spot-checks or inventory by personnel directly responsible for handling of CTS/A classified documents and material.

2-3. **ACO CTS/A Central Registry.** The ACO CTS/A Central Registry established at SHAPE performs the following primary functions:

a. Requests and receives ATOMAL documents from the Government of the United States of America and from other ATOMAL Central Registries, Sub-Registries and CPs.

b. Maintains, for ACO, formal records of all transactions involving ATOMAL documents, by assigning, in a separate paper logbook, unique ACO Control Numbers to each ATOMAL holdings within the ACO CTS/A Registry System.

c. Maintains separate paper logbook for CTS holdings.

d. CTS and ATOMAL logbooks shall be authorised for use by the ACO Security Authority and ACO CACO and when filled in, shall be retained indefinitely (an electronic database may be used as a supporting tool for tracking the CTS and ATOMAL holdings within the ACO CTS/A Registry System).

e. Control access to CTS and ATOMAL information held.

f. Transfers CTS and ATOMAL documents to CTS/A Central Registries and authorised CTS/A Sub-Registries and CPs in other NATO components and to ACO component CTS/A Sub-Registries and CPs.

g. Maintains, for SHAPE, the current lists of individuals, provided by the SHAPE CACO who have been authorised to access CTS and ATOMAL information based on the NTK principle.

h. Advises the ACO Security Authority through SHAPE CACO and ACO CACO on establishment and/or dis-establishment of CPs under its direct authority.

i. Maintains record of subordinated CPs located within the SHAPE compound.

j. Maintains records of all ACO component CTS/A Sub-Registries and CPs.

k. Maintains a hard copy (paper) of all records of CTS and ATOMAL Central Registries, Sub-Registries and CPs of other NATO components with which it, or ACO component CTS/A Sub-Registries or CPs, are authorised to exchange CTS and ATOMAL information.

l. Performs the co-ordination of access to CTS and ATOMAL information with Special Limitations and exchange of receipts within 30 days of sending and receiving CTS or ATOMAL information.

m. Destroys CTS and ATOMAL information by authorised means.

2-4. **ACO Component CTS/A Sub-Registries.** ACO component CTS/A Sub-Registries perform the following primary functions:

a. Receive CTS and ATOMAL documents from the ACO CTS/A Central Registry;

b. When authorised by the ACO Security Authority:

(1) Receive CTS and ATOMAL documents from other CTS and ATOMAL Sub-Registries and CPs within ACO.

(2) Request and receive such documents from the United States of America and from ATOMAL Central Registries, Sub-Registries and CPs in other NATO components.

c. Maintain records of transactions involving CTS and ATOMAL information.

d. Request the ACO CTS/A Central Registry allocation of the unique ACO Control Number for each and every piece of ATOMAL material originated within the respective ACO component, or received directly from outside ACO CTS/A Registry System.

e. Control access to CTS and ATOMAL information held.

f. Transmit CTS and ATOMAL documents to an ACO CTS/A Central Registry and, when authorised by the Security Authority, to CTS/A Sub-Registries and CPs within the ACO components.

g. When authorised, transmit CTS and ATOMAL documents to authorised CTS/A Central Registries, Sub-Registries and CPs in other NATO components.

h. Maintain current lists of individuals who have been authorised by the Security Authority to access CTS and ATOMAL information based on a need-to-know. The list is provided by HQ CACOs.

i. When authorised, advise the Security Authorities through HQ CACOs on establishment or disestablishment of CPs under their direct authority.

j. Maintain records of those CTS/A Sub-Registries and CPs, of other NATO components, with which it or its subordinate CPs are authorised to exchange CTS and ATOMAL information directly, together with specimen signatures of control personnel.

k. Perform co-ordination of access to CTS and ATOMAL information with Special Limitations and exchange of receipts within 30 days of receiving CTS or ATOMAL information.

l. Destroy CTS and ATOMAL information, by authorised means, when authorised by the ACO CTS/A Central Registry and HQ CACOs.

2-5. Within the ACO CTS and ATOMAL Registry System establish CPs, which are categorised as follows:

a. Category 1 CPs are established to serve the subordinate ACO components, or activities, located outside of the physical premises of the parent headquarters.

b. Category 2 CPs are established within the parent ACO component headquarters or activities and serve one or more staff elements.

2-6. **CPs perform the following primary functions:**

a. Receive CTS and ATOMAL documents from the ACO CTS/A Central Registry or from other ACO component CTS/A Sub-Registries and, when authorised by the Security Authority, request and receive such documents from other NATO components CTS/A Central Registries, Sub-Registries and CPs.

b. Control access to CTS and ATOMAL information held.

c. Maintain records of transactions involving CTS and ATOMAL information.

d. Transmit CTS and ATOMAL documents to the ACO CTS/A Central Registry or parent CTS/A Sub-Registry and, when authorised by the ACO Security Authority, to other ACO component CTS/A Sub-Registries and CPs, or other NATO component CTS/A Central Registries, Sub-Registries and CPs.

e. Maintain, for the ACO component served directly by the CP, current lists of individuals (provided by HQ CACOs), who have been authorised, by the Security Authority, to access CTS and ATOMAL information based on the need-to-know principle.

f. Forward CTS and ATOMAL documents to the ACO CTS/A Central Registry or to their parent ACO component CTS/A Sub-Registry when no longer needed.

g. Maintain, records, provided by HQ CACOs, of those CTS/A Sub-Registries and CPs of other NATO components with which it is authorised by the Security Authority to exchange CTS and ATOMAL information directly, together with specimen signatures of control personnel.

h. When authorised by the Security Authority, perform in co-ordination with HQ CACOs, access to CTS and ATOMAL information with Special Limitations and exchange of receipts within 30 days of receiving CTS and ATOMAL information.

2-7. **ACO Security Authority.** The ACO Security Authority is responsible for the CTS and ATOMAL security programme within ACO. This authority is further discharged for all the ACO components.

2-8. **Dissemination of CTS and ATOMAL Information within ACO**

a. In the absence of Special Limitations precluding such dissemination, any ACO component receiving CTS or ATOMAL information in documents, electronically, orally or visually may disseminate the information to individuals (including the personnel to whom access is authorised for administrative reasons) within the component who possess personnel security clearances and who are determined to have a need-to-know by the components' Security Authority.

b. Within each ACO component separate accountability records and storage of CTS and ATOMAL information shall be exercised by the CTS/A Central Registry, ACO component CTS/A Sub-Registries and CPs, to limit access to such information to authorised personnel only.

2-9. Dissemination of CTS and ATOMAL Information between ACO and Other NATO Components

a. In the absence of Special Limitations precluding such dissemination, CTS and ATOMAL information will be exchanged through ACO CTS/A Central Registry and ACO component CTS/A Sub-Registries and CPs. A list of ATOMAL Central Registries of each NATO component is at Annex H.

b. Each ACO component shall, through the ACO CTS/A Central Registry and ACO CACO, keep the NOS informed of the identity of all its CTS/A Sub-Registries and CPs authorised to request, transmit and receive CTS and ATOMAL information directly from other NATO components. ACO component HQ CACOs shall advise other appropriate NATO components of these designations. Specimen signatures of authorised registry CCOs shall be exchanged between the ACO CTS/A Central Registry, ACO component CTS/A Sub-Registries and CPs and authorised Central Registries, Sub-Registries and CPs of other NATO components.

c. When a transmission is made to a CTS/A Sub-Registry or CP within ACO, or to a Sub-Registry or CP of another NATO component, the sender shall at the same time, or as soon as possible and in no case later than 30 days thereafter, provide the ACO CTS/A Central Registry or another NATO component CTS/A Central Registry of the receiving component, either with the information transmitted if it has been requested or with the reference numbers making it possible to identify without error the documents containing the information required. Transmissions of CTS and ATOMAL information within ACO or to another NATO component shall be limited to those instances in which the sender determines the receiver has a need-to-know in connection with a NATO mission. The ACO component receiving such information is responsible for its safeguarding, controlling, accounting and reporting in accordance with this directive.

d. When a transmission of CTS and ATOMAL information is made outside of the ACO CTS/A Registry System, the receipt and courier certificate confirming such transmission shall be retained by ACO CTS/A Registry System elements indefinitely.

2-10. Control of COSMIC TOP SECRET and ATOMAL Documents

a. Incoming CTS and ATOMAL documents shall be received in the ACO CTS/A Central Registry, ACO component CTS/A Sub-Registries and CPs. Such documents are to be processed by designated registry CCOs, DCOs or alternates only.

b. All CTS and ATOMAL documents shall be controlled by the ACO CTS/A Central Registry, ACO component CTS/A Sub-Registries and CPs.

c. After completion of administrative processing, each CTS and ATOMAL document shall be kept within a Class I Security Area in a specially-dedicated security container; the authorised action officer shall be notified that the document has been inventoried and is ready to be reviewed.

d. Control of CTS and ATOMAL documents shall be maintained by a continuous chain of receipts.

e. Each CTS and ATOMAL document shall be kept in a separate colour coded folder, together with accompanying documentation created during its life cycle.

f. All draft papers, resulting from the preparation of CTS and ATOMAL documents, shall be delivered to the ACO CTS/A Central Registry or to ACO component CTS/A Sub-Registry for destruction.

2-11. **Page Checking.** Page checking of CTS and ATOMAL documents shall be carried out as follows:

a. Immediately upon receipt of a new CTS and ATOMAL document.

b. Upon rotation of the Supervisor of the ACO CTS/A Central Registry, ACO component CTS/A Sub-Registry or CP.

c. Upon ACO CTS/A Central Registry, ACO component CTS/A Sub-Registry or CP receipt of a CTS and ATOMAL document previously held by the Action Officer.

d. Upon entering a change (other than pen and ink) into a CTS and ATOMAL document.

e. During the course of the annual inventory of CTS and ATOMAL documents.

f. During the course of the quarterly 25% spot-checks of CTS and ATOMAL documents, conducted by HQ CACO.

2-12. **Classification of ATOMAL Information**

a. Security classification as applied, by either the Government of the United States of America or the Government of the United Kingdom, according to the origin of the information, to ATOMAL information communicated under the Agreement shall be observed at all times.

b. The Classification of reproductions shall be as high as that of the original document or of the separately classified portions reproduced, unless otherwise authorised by either the Government of the United States of America or the Government of the United Kingdom.

c. In the absence of specific classification guidance from the Government of the United States of America and/or from the Government of the United Kingdom, classification of generated documents shall be at least as high as the documents (separately classified portions) from which the information in the generated documents was derived.

d. Questions pertaining to classification of information shall be referred, as appropriate, to the Government of the United States of America and/or the Government of the United Kingdom, depending on the origin of the information.

2-13. **Marking of Documents.** All documents containing ATOMAL information shall be marked as follows:

a. “COSMIC TOP SECRET – ATOMAL”, “NATO SECRET – ATOMAL” or “NATO CONFIDENTIAL – ATOMAL”, as appropriate, shall be placed at the top and bottom of each page.

b. One of the following statements, as appropriate, shall be placed on the face of the document:

EITHER

(1) “This document contains United States atomic information (Restricted Data or Formerly Restricted Data) made available pursuant to the NATO Agreement for Co-operation Regarding Atomic information dated 18 June 1964 and will be safeguarded accordingly;”

OR

(2) “This document contains UK ATOMIC information. This is released to the North Atlantic Treaty Organisation including its military and civilian agencies and member states on conditions that it will not be released by the recipient organisation to any other organisation without prior permission from HM Government of the United Kingdom,”

OR

(3) In the case of generated documents containing atomic information originating from both United States and United Kingdom, both statements prescribed in sub-paragraph 2-9b(1) and 2-9b(2) shall be placed on the face of the document

c. Documents released under Special Limitations shall be appropriately marked on the face of the document to indicate the limitation that has been imposed by the United States and/or by the United Kingdom Government, as appropriate.

d. Where reproductions of, or generations from, an ATOMAL document are not authorised, the document will bear a notation to that effect.

e. For accountability purposes, each ATOMAL document must bear a unique reference number and date and each copy must be copy-numbered. Additional markings for accountability purposes may be used as appropriate.

f. In electronic communications, “COSMIC TOP SECRET – ATOMAL”, “NATO SECRET – ATOMAL” or “NATO CONFIDENTIAL – ATOMAL”, as appropriate, shall be transmitted at the beginning of each message followed by a reference to any Special Limitations which are applicable. When the text of the message appears in documentary form, it shall be marked in the same manner as other ATOMAL documents.

g. Component parts (e.g. paragraphs and titles) of ATOMAL documents issued henceforth shall bear individual classification markings.

h. Holders of documents containing ATOMAL information which have been issued without the ATOMAL markings shall mark these documents as indicated above when notified that such documents are ATOMAL. When so notified, a review

shall be made to determine if any reproductions of these documents have been made and whether any generated documents based on ATOMAL information derived there from have been prepared and, if so, they shall be marked as indicated above.

i. Any holders who believe that a NATO document in their custody, not bearing ATOMAL markings, contains ATOMAL information, shall safeguard the document as ATOMAL and request clarification and guidance from the originator of the document.

j. When originators determine that documents containing ATOMAL information are not properly marked, they shall place the documents under controls prescribed herein, apply the ATOMAL markings and advise all recipients to which copies of the documents have been transmitted accordingly. The ACO CTS/A Central Registry, ACO component CTS/A Sub-Registries and CPs receiving such notification shall take the same action and in turn advise subsequent recipients.

k. Questions regarding the ATOMAL content of documents shall be referred to the Government of the United States and/or the United Kingdom, according to the origin of the information held therein.

2-14. **Personnel Security Clearances.** The granting of a PSC and the specification of the classification level to which the individual is cleared is a function of responsible government authorities of the individual's parent nation. Copies of these PSCCs shall be held by the ACO component to which the individual is assigned.

2-15. **Access.** Access to particular CTS and ATOMAL information shall be governed by the Security Authority, by the level of PSC the individual holds, as granted by his/her government, and by the NTK principle. Access to CTS and ATOMAL information shall be annually, up to 30 September each year, determined by the HQ CACO of the ACO component to which the individual is assigned; this will also be subject to any Special Limitations on dissemination that may exist. HQ CACO's shall provide the ACO CTS/A Central Registry, ACO components Sub-Registry and CPs with current lists of individuals within its sphere of operation who have been granted, by the relevant Security Authority, access to CTS and ATOMAL information (separate for CTS and for ATOMAL). Such lists shall also specify those individuals who have authorised access to ATOMAL information released under Special Limitations. 'Exceptional circumstances' provisions for access to NCI do not apply to ATOMAL information.

2-16. **Disclosure Record.** A disclosure record sheet shall be affixed by the ACO CTS/A Central Registry, ACO component Sub-Registry and CPs to CTS, CTS/A and to NS ATOMAL documents, as well as to NC ATOMAL documents on which Special Limitations have been placed. All persons who have had access to, and knowledge of, the content of such documents shall sign the disclosure record sheet (see Annex I). When the document is destroyed, the disclosure sheet shall be removed and retained indefinitely along with a copy of the Destruction Certificate (ACO Form 99) in the permanent files of the ACO CTS/A Central Registry, or ACO component CTS/A Sub-Registry.

2-17. **Accountability.** The ACO CTS/A Central Registry, ACO component Sub-Registry and CPs shall maintain records of receipt, reproduction, generation, transmission, change of classification, and destruction for all CTS and ATOMAL documents. Accountability records for ATOMAL documents shall be maintained separately from the records

controlling CTS documents. These records shall also clearly identify those ATOMAL documents which contain UK ATOMIC information. Accountability records for CTS and ATOMAL documents shall be retained indefinitely after the transfer or destruction of the CTS or ATOMAL document.

2-18. **Reproductions:**

a. NS ATOMAL and NC ATOMAL documents not subject to Special Limitations that are released by the United States of America to an ACO component, may be reproduced by the ACO component in limited numbers to satisfy bona fide requirements, subject to prior authorisation by the ACO component HQ CACO. NS ATOMAL and NC ATOMAL documents generated by a NATO component may be reproduced as required, unless specific instructions to the contrary are issued by the originating NATO component. CTS/A and all ATOMAL documents subject to Special Limitations may be reproduced only with the prior approval of the Government of the United States of America.

b. ATOMAL documents containing UK ATOMIC information may not be reproduced unless specific instructions to the contrary are issued by the Government of the United Kingdom.

c. In all cases, reproductions of ATOMAL documents shall bear the markings applicable to the original document or portion reproduced, as set forth in paragraph 2-9 above and shall be accounted for as specified in paragraph 2-13.

2-19. **Generated Documents:**

a. ATOMAL information may be incorporated in generated documents by any NATO component as required unless specific limitations on generation are imposed by the Government of the United States of America and/or the Government of the United Kingdom. Documents not authorised to be used for generation of other documents will bear a notation to that effect.

b. In all cases, generated documents shall be marked as set forth in paragraph 2-9 above and shall be accounted for as specified in paragraph 2-13.

2-20. **Oral and Visual Communications:**

a. ATOMAL information, not under Special Limitations precluding such dissemination, may be communicated orally and visually between personnel listed on the authorised access lists provided that, for purposes of proper protection, there is co-ordination between appropriate ATOMAL Central Registries and, when authorised, Sub-Registries and CP to ensure that the recipients are properly authorised to have access to the information involved. These lists are to be held within the ACO CTS/A Central Registry, ACO component Sub-Registries and CPs in the same ACO component or within different NATO components (See Annex J for visit request procedures).

b. Following each such communication between ACO components or other NATO components, a written or electronic record of any new information exchanged and the names of the recipients shall be prepared by the disseminating ACO component with copies to be provided within 30 days to the receiving

components. The copies to the receiving components shall be sent either to the ATOMAL Central Registries or to the Sub-Registries/CPs servicing the NATO component to which the individual recipients are assigned. Such documents shall be controlled and accounted for in accordance with this regulation.

2-21. **ATOMAL Exercise Documents**

a. ATOMAL information transmitted for the purpose of exercises shall be handled, marked and controlled according to the requirements as prescribed for ATOMAL documents. Accountability records, however, shall be kept separate.

b. Exercise documents shall normally be destroyed no later than 5 days after the completion of the exercise. All control records, destruction certificates, logbooks and index cards, etc., shall be retained in the ACO CTS/A Central Registry, ACO component Sub-Registries or CPs indefinitly.

c. Exercise documents retained for more than 5 days after the completion of the exercise shall be accounted for as any other ATOMAL documents.

2-22. **Disposition.** The ACO CTS/A Central Registry and ACO component Sub-Registries shall develop and implement, under supervision of an ACO component HQ CACO, a programme for the systematic screening of CTS and ATOMAL information under its overall control, in order to determine when the information is no longer required for official purposes; this may include archival retention. If needed, guidance may be sought from the originator of the information. Unless otherwise directed, the information shall not be returned to the originator for destruction and the ACO CTS/A Central Registry shall carry out destruction. ACO component Sub-Registries may carry out destruction when specifically authorised by the ACO CTS/A Central Registry. CTS and ATOMAL information shall be destroyed in such a manner as to ensure that it is beyond recognition or reconstruction. Destruction of CTS and ATOMAL information shall be listed on a Destruction Certificate that shall be signed by the head of ACO CTS/A Central Registry or when authorised by the head of ACO component Sub-Registry and by an ACO component HQ CACO and by an independent witnessing official, who shall be appropriately security cleared and authorised to access the classification of CTS and ATOMAL information being destroyed. Destruction Certificates shall be retained indefinitely after destruction of the related CTS or ATOMAL documents. Specific requirements for a destruction of CTS and ATOMAL Classified Electronic Storage Media/Devices are described in AD 070-005, “ACO CIS Security Directive”. Detailed procedures for the destruction of CTS and ATOMAL Classified Electronic Storage Media/Devices shall be included in ACO Manual 070-001-003 and AD 070-005. Within each ACO CTS/A Registry system a relevant site specific instruction shall be included in local Standard Operational Procedures for the destruction of CTS and ATOMAL Classified Electronic Storage Media/Devices.

2-23. **Security Briefings.** A security briefing programme shall be established within each ACO component and conducted by the relevant DSO for CTS and HQ CACO for ATOMAL information to ensure that all personnel having access to CTS and/or ATOMAL information receive:

a. Prior to access, a special briefing on the applicable security requirements and regulations for protecting CTS and ATOMAL information and sign a certificate to that effect.

b. An annual re-briefing, with signature of a certificate to that effect.

c. A termination briefing stressing continuing security responsibilities for the safeguarding of CTS and ATOMAL information, with the person's signature on a briefing certificate indicating that such a briefing was conducted and that the persons continuing responsibilities are understood.

2-24. **Reports.** An Annual Inventory Report on CTS and ATOMAL information held within elements of ACO CTS/A Registry System, signed by the ACO Security Authority, shall be submitted by 31 March each year by the ACO CACO to the NOS. To facilitate this, all the ACO component HQ CACOs are required to submit, through their Security Authorities, their annual inventory reports to ACO Security Authority by 31 January each year. The annual inventory of CTS and ATOMAL information held by elements of ACO CTS/A Registry System shall be conducted by designated inventory teams. The inventory teams shall be composed of independent, properly security cleared subject matter experts, supported by respective registries' and CPs' control personnel and led by ACO component HQ CACOs. These reports shall contain:

a. A list, by ACO CTS/A Central Registry, ACO component Sub-Registries and CPs of each CTS and ATOMAL items on hand as on 31 December. Each item shall be identified in the report by its NATO/ACO reference number, originator, date, unclassified subject and/or short title, classification and copy number. The same information for each CTS and ATOMAL item received during the reporting period shall be provided, regardless of whether it has been subsequently transferred or destroyed. Negative (nil) reports are required.

b. A certificate, signed by the ACO component Security Authority and by the HQ CACO that a physical muster has been made of all CTS and ATOMAL documents held by the ACO component. Material is regarded as accounted for if:

(1) It is physically sighted and a page count is completed;

(2) A Destruction Certificate is held;

(3) A transfer receipt to another CTS and ATOMAL registry is held; or

(4) A declassification authorisation is held.

c. A list of any CTS and ATOMAL documents unaccounted for, to include missing pages from documents, together with the dates that the immediate reports required by paragraph 1-22 below were made.

2-25. **Inspections.** The inspection programme is the primary instrument for determining the adequacy of compliance with the security arrangements for safeguarding CTS and ATOMAL information:

a. An inspection programme shall be established within each ACO component to ensure that the ACO CTS/A Central Registry and ACO component CTS/A Sub-Registries and CPs holding CTS and ATOMAL information are inspected a minimum of once every 24 months.

b. For those ACO components authorised to hold, but not actually holding, CTS and ATOMAL information, the frequency of inspections will be determined by each ACO component Security Authority. However, the ACO Security Authority shall be assured once every 12 months by ACO component Security Authorities that their relevant Sub-Registries and CPs authorised to hold, but not actually holding, CTS and ATOMAL information have the required security arrangements to protect such information in place, and that such security arrangements continue to be effective.

c. Inspections shall be carried out by qualified personnel and effective and expeditious corrective action shall be taken where required. SACEUR and respective ACO component commanders are responsible for all their subordinate international commands and agencies.

d. Inspection reports, including annual assurances provided to the ACO Security Authority by Security Authorities of the ACO components authorised to hold, but not actually holding CTS and ATOMAL information, shall be sent to the NOS within 30 days after completion of the inspection or receipt of the assurance, through the ACO CACO. There is no need for a separate report on organisations holding UK ATOMIC information.

e. Within 30 days after receipt of the inspection report, the Security Authorities of the ACO components inspected, or Security Authorities of superior ACO components, shall forward to the ACO Security Authority a report of the action taken to correct any deficiencies listed in the inspection report. A copy of corrective action shall be forwarded to the NOS.

2-26. **Breaches of Security and Compromises.** If CTS or ATOMAL information is compromised by loss of documents or any other means, or is believed to have been compromised, an immediate report shall be made by the Security Authority of the ACO component to the ACO Security Authority, copied to the NOS, in accordance with security procedures stipulated in Part VI, Chapter 1 of this directive.

2-27. **Responsibilities**

a. Responsibilities of the ACO CACO. The ACO CACO is appointed by the ACO Security Authority and is responsible for the supervision of the ACO CTS/A Registry System. Specifically:

(1) The security inspection of each element of ACO CTS/A Registry System at least once every 24 months;

(2) For the ACO Security Authority the initiation and coordination, of the Annual Inventory of all CTS and ATOMAL information held within all ACO CTS/A Registry System elements;

(3) Forwarding the combined report on ACO Annual Inventory of ATOMAL information held within the ACO CTS/A Registry System elements to the NOS;

(4) Organising in cooperation with the head of ACO CTS/A Central Registry annual training for the ACO component HQ CACOs, on

requirements of NATO security policy and on the ACO CTS/A Registry System procedures;

(5) Monitoring the results of CTS and ATOMAL 25% spot-checks, which are carried out and delivered quarterly by ACO component HQ CACOs;

(6) Based on results of security inspections and 25% spot-checks, programming and providing security awareness dedicated to ACO component HQ CACOs and CCOs;

(7) Providing ACO personnel guidance and advice on the requirements of NATO security policy with reference to protection of CTS and ATOMAL information;

(8) Provide to the NOS, by the 31 March each year, a current list of ACO CTS/A Registry System elements, authorised to hold ATOMAL information;

(9) Coordinate with ACO component Security Authorities certification procedures of newly established CTS/A Sub-Registries and CPs.

b. Responsibilities of HQ CACO. ACO component HQ CACOs are responsible for the supervision of the relevant elements of ACO CTS/A Registry System within their headquarters. Specifically:

(1) Conducting 25% quarterly spot-checks of CTS and ATOMAL information held by subordinated ACO CTS/A Central Registry, ACO component Sub-Registries and CPs.

(2) Forwarding the list of spot-checked CTS and ATOMAL holdings to the ACO CACO as an integral part of the Quarterly Security Returns.

(3) Initiating and supervising of annual inventory of CTS and ATOMAL information held by ACO CTS/A Central Registry, ACO component Sub-Registries and CPs. This is to be started by 10 November each year and shall be completed by 31 December each year.

(4) Reporting the results of the annual inventory of CTS and ATOMAL information to ACO Security Authority through the HQ Security Authority up to 31 January each year;

(5) Initiate and coordinate annual revision of CTS and ATOMAL information, in order to determine further courses of action.

(6) Supervise the process of destruction of CTS and ATOMAL information.

(7) Provide annually, up to 30 September each year, the ACO CTS/A Central Registry, ACO component Sub-Registries and CPs with lists of personnel, together with their specimen signatures, authorised to access CTS information, ATOMAL information and ATOMAL information with Special Limitations signed by HQ Security Authority.

(8) Supervise the handover/takeover of the head of ACO CTS/A Central Registry and heads of ACO component CTS/A Sub-Registries and CPs.

(9) Brief personnel having access to ATOMAL information prior to initial access and ensure that they sign an In-briefing Certificate affirming their understanding of applicable security regulations (ACO Form 107).

(10) Brief personnel having access to ATOMAL information annually and ensure the signature of a certificate reaffirming their understanding of NATO and local security procedures (ACO Form 107).

(11) Provide personnel having access to ATOMAL information, upon termination of access, a termination de-briefing and ensure the signature of a De-briefing Certificate to the effect that such an interview was conducted and that they understand their continuing responsibilities for the safeguarding of ATOMAL information (connect ACO Form 107).

c. Responsibilities of COSMIC Control Officers. Heads of ACO CTS/A Central Registry, and ACO component CTS/A Sub-Registries shall be appointed in written by relevant Security Authorities as CCOs. Their responsibilities are as follows:

(1) To ensure that all information classified CTS and ATOMAL held by the ACO CTS/A Central Registry and ACO component CTS/A Sub-Registries are physically protected in accordance with NATO standards and local security instructions.

(2) To maintain an up-to-date record of all CTS and ATOMAL material received, held or circulating within the ACO CTS/A Central Registry and ACO CTS/A Sub-Registries or passed to other NATO component CTS/A Central Registries, CTS/A Sub-Registries or CPs and maintain records of disclosure and Destruction Certificates (connect ACO Form 99).

(3) To maintain up-to-date records, by name, of all individuals authorised by ACO component Security Authority access to CTS and ATOMAL information held by its CTS/A Sub-Registry (connect ACO Form 120).

(4) To maintain up-to-date records of all other CTS/A Sub-Registries and CPs with which they are authorised to exchange CTS and ATOMAL information, together with the names of the associated personnel and their specimen signatures.

(5) To maintain and submit to the ACO CTS/A Central Registry and to the authorised CTS/A Sub-Registries of the other NATO components with which they normally correspond, an up-to-date list of the names and specimen signatures of appointed CACO, DCACO and Alternates.

(6) To ensure, before acceptance, that all newly generated or originated CTS and ATOMAL documents has been prepared in accordance with the provisions of this directive and Reference E.

(7) To disseminate CTS and ATOMAL material in accordance with the listings of authorised recipients.

(8) To support the annual inventory of CTS and ATOMAL material held.

(9) To obtain receipts from CTS/A Sub-Registries for all CTS and ATOMAL material distributed.

(10) To report immediately, to the relevant HQ CACO when a receipt is not sent back by the receiving ACO component or NATO component CTS/A Central Registry, Sub-Registry or CP, during 30 days since CTS or ATOMAL information has been transferred.

d. Responsibilities of CP COSMIC Control Officers. Personnel designated to handle and control CTS and ATOMAL information within ACO component CPs, shall be appointed in writing by relevant Security Authorities as CP CCOs. Their responsibilities are as follows:

(1) To ensure that all information classified CTS and ATOMAL held by the CP is physically protected in accordance with NATO standards and local security instructions.

(2) To maintain an up-to-date record of all CTS and ATOMAL material received, held or circulating within the CP and maintain records of disclosure.

(3) To maintain up-to-date records, by name, of all individuals authorised by the ACO component Security Authority access to CTS and ATOMAL information held by the CP (connect ACO Form 120).

(4) To maintain up-to-date records of all other CTS/A Sub-Registries and CPs with which it is authorised to exchange CTS and ATOMAL information, together with the names of the associated CCOs and their specimen signatures.

(5) To ensure, before acceptance, that all newly generated or originated CTS and ATOMAL documents has been prepared in accordance with the provisions of this directive and Reference E.

(6) To disseminate CTS and ATOMAL material in accordance with the listings of authorised recipients.

(7) To support the annual inventory of CTS and ATOMAL material held.

(8) To obtain receipts from CTS/A Sub-Registries for all CTS and ATOMAL material distributed.

(9) To report immediately, to the relevant HQ CACO when receipt is not sent back by receiving ACO component or NATO component CTS/A Central Registry, Sub-Registry or CP, during 30 days since CTS or ATOMAL information has been transferred.

(10) To return all CTS and ATOMAL material to their parent CTS/A Sub-Registry when it is no longer required.

This page is intentionally left blank.

CHAPTER 3 – PREPARATION, TRANSFER, CONTROL AND DESTRUCTION OF CLASSIFIED DOCUMENTS

3-1. Preparation and Display of Security Classifications and Markings:

a. Documents. All documents including permanently bound books, files and pamphlets or reproductions are to have their overall classification conspicuously stamped, typed, printed or handwritten as described in Part III Chapter 1.

b. Charts, Maps and Drawings. The classification of classified charts, maps and drawings is to be marked under the legend, title blocks or scale and on the outside when folded. If a wall display is subject to frequent classification change, an overlay or other such system may be used.

c. Photographic Material. Photographs, films, microfiche, including negatives and positives, and their spools and containers, are to be marked in such a manner to ensure that any recipient or viewer will know that classified information of a specified level is involved. Microfilm is to show the highest classification at the beginning and end of each microfilm reel, including the listing of contents at the beginning of the reel.

d. Tape Recordings. The spools containing tapes, including videotapes, on which classified information has been recorded, are to be clearly marked with the highest classification of information ever recorded. This classification is to remain on the spool until the tape has been destroyed or degaussed by a method approved by a member nation for the declassification of the type of tape involved. When recording, the appropriate classification is to be quoted at the beginning and end of each passage. Each end of classified tapes is to be visibly marked with its classification in case the tapes become detached from their spools. Recordings are to be kept in containers or on spools that bear conspicuous classification markings.

e. Communication and Information Services Products. Special provisions for the marking of CIS products (magnetic tapes, disks, hard drives, flash drives, etc.) are contained in AD 070-005 CIS Security. For proper disposal and destruction methods of classified magnetic media see Annexes K and L.

f. Other Material. The assigned security classification and, where appropriate reclassification instructions, are to be conspicuously stamped, printed, written, painted or affixed by means of a tag, sticker, decal or similar device on classified material other than that described above.

g. Covering Document. A covering document is to bear the classification of either the material it covers or the content of the covering document itself, whichever is the highest. A covering document which may be downgraded when separated from its enclosures is to bear the following statement:

"WHEN SEPARATED FROM CLASSIFIED ENCLOSURES, THIS PAPER SHALL BE HANDLED AS (INSERT APPROPRIATE CLASSIFICATION)"

h. ACO Forms. Some ACO forms are printed with instructions concerning minimum classification requirements when the form is completed. In the absence of such instructions, each form shall be classified according to content.

i. Folders, Files and Covers. Folders, transit covers and files are to be colour coded using the colours shown below:

(1) COSMIC TOP SECRET - Red.

(2) NATO SECRET - Blue.

(3) NATO CONFIDENTIAL - Green.

(4) NATO RESTRICTED - Buff/Yellow.

(5) NATO UNCLASSIFIED - Buff/Yellow or White.

3-2. **Reclassification Marking Procedures.** When a document is reclassified by, or on the authority of the originator, the original NATO classification on the outer cover, title page and first and last pages is to be lined through and the new security classification or NU is to be shown immediately above or below it. The authority for such action, together with the date and signature of the person effecting the amendment, are to be shown on the first page of the document.

3-3. **Aural and Visual Projections of Classified Material.** Classified documents, in the form of recording tapes (including video tapes), films and photographs (developed or undeveloped), projection slides, viewgraphs and similar items are to be prepared, safeguarded and controlled in accordance with the provisions of this directive. When not in use, their containers or covers are to bear the appropriate classification marking and reference or control and copy numbers, if applicable. In addition, special safeguards are to be applied, in order to protect the presentations themselves, as follows:

a. Magnetic Tapes and Video Tapes. The recording is to open with a statement as to classification of the ensuing commentary and, at the end, the classification is to be restated. In the case of videotapes, the classification should, if feasible, appear on the screen as well. If classification cannot accurately be determined before the tapes are made, the appropriate ‘marking’ is to be applied later by the insertion of a separate ‘leader’ and ‘tail’. It is important to note that normal ‘erasure’ of a classified recording does not downgrade or declassify a tape, even though the process is intended to remove the audible signals. Once a tape has been used for a classified recording, it is to retain its highest grading either until it is destroyed, or until its grading is raised by the addition of further recording of higher classification, or it is degaussed by a process approved by the Security Authority.

b. Silent Visual Projections:

(1) Still projections are to show the reference number (or control and copy numbers if applicable), as well as classification. In the case of viewgraphs prepared specifically for a particular presentation or briefing within a situation centre, or similar secure area, and which, because of their transient content, are wiped clean after showing, they need to display only the classification, provided that they remain within the secure area and in the control of their originator(s). If, however, classified viewgraphs are moved out of the custody of their originator(s), then the full control procedures appropriate to their classification are to be applied.

(2) Cine projections are to show the reference number (or control and copy numbers if applicable), as well as classification on the title frames.

3-4. **File Reference Numbers.** All NATO classified documents are to be assigned a file reference number that is to appear on the first page.

3-5. **Dating and Copy Numbering.** All classified documents are to be dated on the first page. CTS, NS and ATOMAL documents are to be copy-numbered on the first page. The distribution list is to show the allocation of copy to individual addressee.

3-6. **Page Numbering and Page Count Details.** All printed or written pages of NATO classified documents are to be numbered consecutively. CTS/NS/ATOMAL are to show the total page count on the first page. Page numbering of all documents is to be in accordance with AD 035-004. If a CTS, NS or ATOMAL document consists of more than one component (e.g. it consists of a basic document plus annexes and appendices), a list of printed pages must be included. As there are different templates used to create documents, page numbering may or may not be present. From the date on which this directive is released, any page that is numbered shall be counted. If no page number is present, it shall not be counted.

3-7. **Additional Copies and Translations.** Additional copies of CTS documents should only be obtained from the originator. Exceptionally; they may be copied or translated on the authority of the HQ CACO. Security measures are to be applied to such reproductions and translations as follows:

a. Bear the reference, copy number and control number of the original document.

b. Show the name of the originating authority and the ACO component reproducing the document. Translations are to be identified as such on the first page.

c. Display the CTS classification and all other original markings.

d. Be marked with an additional locally assigned copy number.

e. Be recorded and distributed through the ACO CTS/A Registry System.

3-8. Reproductions, extracts and translations of information classified NS and below may be produced by the addressee under strict observation of the need-to-know principle. Security measures laid down for the original document shall be applied to such extracts, reproductions and/or translations. Reproductions, extracts and translations of information classified NS shall be marked with identifying copy numbers, and the numbers shall be recorded in the responsible ACO registry reproductions, extracts and translations of information classified NC and NR may be produced by the addressee provided they are controlled in a manner to deter unauthorised access. Any extract from a classified document shall bear the NATO security classification of the document or component thereof (if individually classified) from which it was taken. In circumstances where there is uncertainty regarding the appropriate NATO security classification of the extract, the matter shall be referred, in writing, to the originator for determination of the correct NATO security classification.

3-9. All NATO classified working papers shall be dated and marked with their NATO security classification. Where drafts, working papers and personal print-outs classified NS (and any reproductions thereof) are originated by individuals, sections or divisions, they do not need to be registered and controlled unless they are to be passed outside of the originating division or office, thereby transferring the responsibility for the protection from the originators. However, these documents shall become accountable after a maximum of 5 working days from the date of origin. If after this period they are still required for current work, they shall be registered within the registry system and charged to the individual.

3-10. Where necessary and when originator consent has been obtained, extracts of NCI may be included in documents when there is positive determination of the need-to-know principle regarding the access by individuals within ACO components who have not previously been authorised access to NCI. In these circumstances, such individuals shall hold an appropriate in-date PSC.

3-11. If, however, the originator of a NATO classified document wishes to control the further dissemination of information contained therein, the originator shall clearly indicate these special limitations with a note stating, for example: “Reproduction of this document in whole or in part, is prohibited unless authorised by the originator” or “Reproduction of paragraphs …to ….annexes…and….is prohibited unless authorised by the originator”. These special restrictions should be applied with discrimination and as infrequent as possible.

3-12. Notwithstanding any originator control limitations, if a document needs to be translated into a language of a NATO Nation the translated document shall retain the original marking, meet all the criteria above regarding reproduction or extraction, and be afforded the same degree of protection as the original. If information classified CTS needs to be translated, the consent of originator shall be obtained.

3-13. Information classified CTS shall not be reproduced or extracted, except when required for translation described above. Additionally, in exceptional circumstances, paper reproductions, extracts or translations of information classified CTS, including extracts and reproductions to or from machine readable media[12], may be made for urgent mission purposes, provided that the reproductions, extracts or translations:

a. Are authorised by the relevant ACO component HQ CACO.

b. Are reported to the ACO CTS/A Central Registry or ACO component CTS/A Sub-registry or CP, which shall maintain a record of the number of reproductions made.

c. Bear the references and copy number of the original information, together with the name of the originator and that of the reproducing ACO CTS/A Central Registry, or ACO component CTS/A Sub-registry or CP.

d. Are marked with an identifying reproduction copy number locally assigned by the body making reproduction or translation.

e. Display the CTS marking and all other markings of the original information.

[12] Machine Readable Media is a medium that can convey data to a given sensing device.

f. Are brought under COSMIC registry control, distributed through COSMIC registry channels and reported in the annual inventory, along with other information classified CTS.

3-14. Where, for operational or mission critical reasons, the requirements set out above cannot be immediately met, the officer in charge of a communication centre[13] may authorise the production of those reproductions and translations necessary to make initial distribution of signals/messages classified CTS. A record shall be made of the number of reproductions and translations made together with a list of recipients. Thereafter, the authority for authorisation of reproduction and translation of the signal/message will be the HQ CACO.

3-15. Reproductions, extracts and translations of information classified NS, including reproductions to or from machine readable media, may be produced by the addressee when necessary for operational or mission purposes, provided that the reproductions and/or translations, including copy numbers, are recorded by the responsible ACO component registry. In circumstances when the registry is not available, a record shall be made by the addressee and forwarded to the appropriate registry as soon as possible.

3-16. Equipment, such as copiers, printers, MFD machines, facsimile equipment and CIS, accredited for use in the reproduction (or transmission) of NCI, shall be physically protected to ensure that only authorised individuals can use or access them.

3-17. **Microfilming and Reproduction from Microfilm.** For emergency destruction purposes or to minimise storage problems, NATO classified documents may be microfilmed, stored on optical disks and magnetic storage media, provided that:

a. The microfilms, optical disks or magnetic storage media are given security protection appropriate to the highest classification of material contained on it.

b. Microfilming of CTS documents is authorised by the HQ CACO. Appropriate records are maintained for all CTS and NS documents.

c. Copies of documents reproduced from microfilm, optical disk or magnetic storage media are to comply with the provisions Part V Chapter 4.

3-18. **Transfer of NATO Classified Material.** The purpose of security during physical transfer of NATO classified documents and material is to ensure appropriate protection against unauthorised observation, modification or disclosure (deliberate or inadvertent).

3-19. For the purpose of this Directive the term ‘transfer of information’ refers to moving NCI and material from one point to one or more other points by physical means.

3-20. As a general principle and whenever possible, the use of secure electronic means is preferred over the use of physical transfer of NCI. All CIS handling NCI shall be subject of a security accreditation process by the relevant Security Accreditation Authority.

3-21. **Hand carriage.** ACO component staff assigned to hand-carry information classified NC and above shall be appropriately security cleared. Such staff shall be briefed by

[13] Communication Centre is an organisation responsible for handling and controlling communications traffic, normally comprising a message centre, a cryptographic centre and transmitting and receiving stations.

relevant security personnel (e.g. Installation Security Officer or ACO Programme/Project Office's Security Manager) on NATO security procedures and shall be instructed on their duties for protecting the NCI entrusted to them.

3-22. **Couriers/Guards/Escorts.** When individuals such as guards and escorts are employed for the transfer of NCI and/or material, or in circumstances where they might have inadvertent or unauthorised access to NCI, they shall be security cleared to the level deemed appropriate by the relevant security authority.

3-23. **Internal Transfer within Establishments of ACO components.** NCI carried by staff within the perimeter of an establishment of ACO component HQ shall be covered in order to prevent observation of its contents. ACO component HQs shall, within their supplements to this Directive, define appropriate security procedures for transfer of NATO classified documents and material outside of Class I or Class II Security Areas and Administrative Zones.

3-24. **Transfer outside of ACO component Establishment within a NATO Nation.** When NCI is sent outside of an establishment of an ACO component within a NATO Nation, the packing requirements described in paragraph 3-25 shall be applied. The physical transfer of NCI within a NATO Nation shall be by the following means:

a. ACO Courier Service – for information classified up to and including CTS and ATOMAL. NOTE: this is the only accepted means for the transfer of information classified CTS and ATOMAL category.

b. National Postal Service – if permitted by national laws and regulations, and if approved by the ACO component Security Authority, information classified up to and including NS may be transmitted by a national postal service.

c. Commercial Courier Service - if permitted by national laws and regulations, and if approved by ACO component Security Authority, such services may be used for information classified up to and including NS.

d. Hand Carriage - if permitted by national laws and regulations, and if approved by the ACO component Installation Security Officer or by the ACO Programme/Project/Construction Office's Security Manager (APOSM), information classified up to and including NS may be transferred by hand carriage by a member of staff or contractor, acting as a courier, with an appropriate level of PSC, provided that:

(1) A record shall be kept in the appropriate ACO component registry or CP of all accountable NCI carried.

(2) NCI shall be packed in accordance with the requirements of paragraph 3-25, and the locked briefcase or other approved security container shall be of such size and weight that it can be retained in the personal possession of the courier.

(3) NCI shall not leave the possession of the courier unless it is stored in accordance with the prescribed requirements. Moreover, it shall not be left unattended, nor shall not be opened en route.

(4) NCI shall not be read in public places.

(5) The courier shall be briefed on their security responsibilities and be provided with a formal written authorisation, in accordance with national laws and regulations.

(6) Within ACO components the hand carriage of information classified NC and NS by staff shall be allowed only in exceptional circumstances (e.g. when individuals are required to travel at a short notice, or when time does not permit such information to be sent by approved secure means, and when reproductions cannot be made available locally at the receiving location). The individual acting as a courier shall be briefed by the ACO component Installation Security Officer or by the ACO Programme/Project Office's Security Manager on their security responsibilities, and be provided with a formal written authorisation in the form of a Courier Certificate.

3-25. Information classified NC and above transferred between sites or establishments shall be packed so that it is protected from unauthorised or inadvertent disclosure. The following standards shall apply:

a. It shall be enclosed in two opaque and strong covers. For NS and CTS a tamper-evident secure envelope, a locked pouch, locked box or sealed diplomatic pouch may be considered as the outer cover.

b. The inner cover shall be secured, bear the appropriate NATO security classification, as well as other prescribed markings and warning terms, and bear the full designation and address of the intended recipient.

c. The outer cover shall bear the designation and address of the intended recipient and a mechanism for proof of delivery for receipting purposes.

d. The outer cover shall not indicate the NATO security classification of the contents, or reveal that it contains NCI.

e. If the NCI or material is hand-carried by courier, the outer cover shall be clearly marked with 'By Courier Only'.

3-26. Information classified as a NR document or material shall, as minimum, be transmitted in a single opaque envelope or wrapping. The markings on the package shall not reveal that it contains information or material classified NR.

3-27. **Transfer between the territories of NATO Nations.** Within ACO components the international transfer of information and material classified CTS shall be by ACO Courier Service only.

3-28. Within ACO components the international transfer of information and material classified NS shall be by ACO Courier Service or hand carriage.

3-29. The use of national postal services for international transfer of information or material classified up to and including NS may be used provided that the NSAs/DSAs of the relevant Nations have a suitable bilateral agreement/arrangement in place in order to support such means of transfer. Within ACO components the use of national postal

services for international transfer of information or material classified up to and including NS is recommended for transfers related to ACO led classified programmes/projects.

3-30. Commercial Services may be used for international transfer of information or material classified up to and including NC provided that the commercial service provider has been approved for such purpose by its NSA/DSA. The recipient should be notified in advance of such a shipment taking place. As a minimum a commercial service shall provide the possibility to track the shipment from the sender to the recipient and provide the sender with proof of delivery. NOTE: this is the recommended means for the transfer of NCI related to ACO component led classified programmes/projects/constructions.

3-31. The following requirements shall be met when information classified NC and above is hand carried by nominated ACO component staff:

a. The package shall bear an official NATO Seal, or be packed in the manner to indicate that it is an official consignment, and should not undergo customs or security scrutiny.

b. The courier shall carry a Courier Certificate recognised by all NATO Nations identifying the package and authorising them to carry the package. As minimum, the courier shall be briefed on his security responsibilities.

c. The courier travel arrangements shall be in accordance with the following restrictions on destinations, routes and means of transportation or, if national regulations are more stringent, in accordance with national regulations:

(1) The courier shall not travel to, through or over non-NATO nations, nor use any means of transportation or any transportation carrier registered in a non-NATO nation, to which any of criteria listed below apply:

(a) The government of the nation:

1/ Has given evidence by word or deed of an attitude hostile to NATO and/or NATO Nations;

2/ Is not able to give a generally agreed level of protection to the life and/or personal belongings of its residents and/or visiting foreigners; or

3/ Has given evidence that it does not respect at all times the immunity of a NATO Seal (connect para 3-34)

(b) The intelligence services of the nation target NATO and/or NATO Nations; or

(c) The nation is at war, or is subject to serious civil unrest.

3-32. In exceptional cases, the above restrictions may be waived by the ACO component security authority, if urgent operational requirements cannot be otherwise met.

3-33. Transfer outside of the territory of NATO Nations of information classified up to and including NS shall be by ACO Courier Service or hand carriage.

3-34. **NATO Seals and Courier Seals.** NATO seals and courier certificates are to be used when NATO classified material graded NC and above is to be transferred across international boundaries between NATO member countries. The seals, pouches and the certificates, which are recognised by NATO Nations but not by other nations, authorise members of NATO organisations to carry sealed packages and across national frontiers without customs examination. An ACO component commander possessing a NATO Seal is to designate, in writing, an officer as the custodian. The custodian, who may appoint other responsible assistants, is to establish precise safeguards to prevent any abuse of the immunity afforded by the seal. Physical security equivalent to those for SECRET material is to be established for NATO Seals. All components of the NATO seals must be issued with a NS control number and NATO seals must be mustered in the same manner as a CTS document. The custodian must sign for the seals and any transmission must be recorded as a NS document. Return of the NATO seals to the NOS must be done through the ACO CTS/A Central Registry. When a NATO seal is used, a NATO courier certificate (see Part VIII, ACO Form 71) is also to be used by official couriers and designated messengers.

3-35. **Special Transmission Procedures.** Electronically transmitted messages classified NC and above are to be encrypted. NR messages are to be encrypted when transmitted outside of the sending ACO component. NR messages are also to be encrypted when transmitted nationally, except where speed is of paramount importance and the means of encryption are not available; in such cases, NR messages may be passed in clear text provided national security regulations so allow. Electronically transmitted messages are to be subject to the following conditions:

a. Only cryptographic systems specifically authorised by the NATO Military Committee are to be used for CTS and NS messages. Nationally approved cryptographic systems may be used for the encryption of NC and NR messages.

b. Under certain exceptional circumstances, such as during impending or actual terrorist activities or during impending or actual hostilities, when speed of delivery is so essential that time cannot be spared for encryption and it is considered that the transmitted information cannot be acted upon by the opposition in time to influence current operations, NR, NC and NS information may be transmitted in clear text provided each occasion is authorised by the commander of the originating ACO component.

c. Messages are to be accorded at least equivalent protection to that laid down for other documents of the same classification. The handling of CTS messages in Signals Centres is to be restricted to specially designated communications personnel whose numbers are to be kept to a minimum.

3-36. **Control of Classified Documents.**

a. Dissemination of NCI shall be on a need-to-know basis. The dissemination of information classified NC and above shall be restricted to individuals who have the appropriate level of PSC, who have been briefed on their security responsibilities, and who are authorised to have access to such information. NR may be disseminated to individuals who have been informed of the prescribed control measures, have been briefed and have a need-to-know for official purposes. Limitations and Disclosure Restrictions. The following classified material has limitations and disclosure restrictions:

(1) COSMIC TOP SECRET Documents:

(a) Each CTS document originated in ACO component should contain a statement authorising local reproduction, translation or further generation of COSMIC documents, or instructions forbidding reproduction, translation or generation in whole or in part.

(b) Originators should place such restrictions on the distribution of CTS documents as are appropriate. Such restrictions are to be contained in the text of each document.

(2) ATOMAL Documents:

(a) In accordance with Article VI of the 1964 ATOMAL Agreement, special limitations on oral, visual and documentary transmission of ATOMAL information may be prescribed by the United States or the United Kingdom. Such limitations are indicated normally by means of appropriate markings on the face of the document and are to be adhered to throughout ACO (see Part III, Chapter 2, Para 2-1 and subparagraphs).

(b) Each ATOMAL document generated within ACO will contain at least one of the statements contained in sub-paragraphs (a) and (b) as well as a comment as indicated in sub-paragraph (c) below:

(c) As the first paragraph of the document: “This document contains United States ATOMIC information (Restricted Data or Formerly Restricted Data) made available pursuant to the NATO Agreement for Cooperation Regarding Safeguarding ATOMIC Information, dated 18 June 1964, and will be safeguarded accordingly.”

(d) As the first paragraph of the document: “This document contains UK ATOMIC Information. This information is released to the North Atlantic Treaty Organisation including its military and civilian agencies and member states on condition it will not be released by the recipient organisation to any other organisation or government or national of another country or member of any other organisation without prior permission from HM Government in the United Kingdom”.

(e) A statement concerning authority to reproduce, translate or generate further ATOMAL documents, or instructions forbidding reproduction, translation or generation in whole or in part, is to appear with the downgrading instructions.

3-37. **Disclosure Control Records for COSMIC TOP SECRET and certain 'Special Limitations' Document:**

a. Each CTS, CTS/A, NS ATOMAL and NC ATOMAL document upon which 'SPECIAL LIMITATIONS' have been imposed (except those covered by paragraph 3-16.b. (2) 5/. above), received or generated within ACO will have a Disclosure Control Record (ACO Form 78) (see Part VIII, ACO Form 78) affixed to it by the office which receives or generates such a document. This includes drafts and working papers when they leave the custody of the originating staff officer. This requirement applies also to exercise documents.

b. The ACO Form 78 will be attached to the cover or first page of the document and will:

(1) Clearly and completely identify the CTS and ATOMAL document attached.

(2) Indicate the names of persons to whom the contents of the document have been disclosed, with the dates of disclosure, this includes the specific administrative personnel processing the document. The ACO Form 78 is to be completed as directed above on initial access and at the time of the annual inventory.

(3) Be completed by the person having custody of the document upon receipt whether the contents of the document has been individually reviewed or not.

c. The following categories need not be included on the ACO Form 78:

(1) Personnel with authorised access to the container housing the document, but who have not been required to view the contents of the document.

(2) All communications centre personnel who each day handle a large volume of such information. A designated representative of the communications centre on behalf of all personnel in the communications centre who may have processed the document will sign the required ACO Form 78.

d. When a CTS and ATOMAL or Special Limitations document is permanently transferred away from the original receiving headquarters or staff division/agency, the original ACO Form 78 will accompany the document. A locally reproduced copy of the ACO Form 78 will be filed with the receipt for the document.

e. When such an ATOMAL document is destroyed, ACO Form 78 will be removed from the document and filed with the destruction certificate.

f. ACO component Commanders are responsible for ensuring that all personnel under their command, who are involved with the handling of ATOMAL material are cognisant of the fact that not all NATO member nations are permitted access to ATOMAL information, regardless of the security clearance level granted by the member nations.

3-38. **Control Numbers – COSMIC and ATOMAL Documents.** All COSMIC and ATOMAL documents received by ACO component headquarters shall normally be controlled under the control number used by the originator. Documents received without the originator's control number shall be allotted a local control number.

3-39. **Accountability.** All material classified NS and above is accountable and all ACO component Commanders are to lay down procedures to ensure such accountability at all stages in the life cycle of these documents. In particular, it is important that document records are carefully maintained and show sufficient detail to allow positive identification of all accountable documents. All accountable documents shall be allocated a unique control number. Separate control logs for the assignment of control numbers are to be maintained for CTS, NS and ATOMAL. The templates and details of the logbooks required for ACO components can be found in AD 070-001-003 ACO CTS and the ATOMAL Registry SOP.

3-40. **Receipting and Page Numbering of Classified Material.** All transactions involving CTS, NS and ATOMAL material are to be effected by signed receipts. Receipts require no security classification unless they themselves contain classified information and, for CTS and ATOMAL documents, are to include the control number, copy number, number of pages, and date of the document. The signatory of receipts for these documents is to ensure that page count is correct. Receipts for NS material are to list the file reference number, copy number and date of the document. Page counting of NS documents and below is not necessary at every stage during transmission by authorised secure means, but is to be conducted by the final recipient. Receipts for ATOMAL documents are to form a permanent record; those for CTS documents are to be retained indefinitely, and for NS documents, for 5 years from the date of the final transaction (i.e. destruction or permanent transfer out of the HQ, Division, Directorate, Branch, etc.). Only the CCO, Deputy CCO or one of designated alternates may sign for CTS or ATOMAL material received.

3-41. **Page Checking.** The final recipient of a NC and above NATO classified document is to ensure that a page count is carried out and is to certify against the page count details on the first page that the page count is correct, adding the date and his signature. If the page count is found to be incorrect, action is to be taken in accordance with Part VI, Chapter 1 of this directive.

3-42. **Receipts for NATO CONFIDENTIAL/NATO RESTRICTED.** Transactions involving NC material need not be covered by receipts except when specifically required by the originator or when handled by official courier who will obtain receipts against package or envelope numbers. No receipts are required for NR material.

3-43. **Control of Classified Working Papers.** All classified working papers (DRAFTS) are to be marked with the appropriate security classification and are also to be annotated 'WORKING PAPER' or 'DRAFT'. All such papers are to be safeguarded according to their classification. All CTS, NATO SECRET and ATOMAL working papers are the personal responsibility of the drafter until they are brought under formal control: this is to be done within 5 working days. After this period, the material must be brought under proper control either at the appropriate ACO component registry, or the ACO CTS/A Central Registry (ATOMAL). Working papers may be distributed internally within a Class II Security Area against receipt, but may not be further distributed or removed unless brought under formal control.

3-44. **Changes to Classified Documents.** Apart from minor corrections, all changes to classified documents are to be made by the substitution of new pages. Changes to CTS, NS and ATOMAL documents are to be disseminated and controlled as separate documents until they are incorporated into the original document. All changes to both CTS and ATOMAL documents are to be processed through the ACO CTS/A Registry system and assigned a control number when appropriate.

3-45. Residual pages arising from such changes are accountable classified documents and must be disposed of in accordance with Paragraphs 3-48 to 3-56. The destruction certificates should indicate the change number and identify all pages individually.

3-46. **Physical Musters and Spot Checks:**

a. General. ACO component commanders are responsible for developing a system of musters and spot-checks to ensure that all accountable material, including messages, held on charge at the headquarters is accounted for. In this context, material is regarded as being mustered when:

(1) It is physically located and a page count is completed.

(2) Destruction has been recorded on a fully completed certificate.

(3) For documents other than ATOMAL, a competent authority has authorised downgrading documents to below NS or declassification. The headquarters has been relieved of accountability for the document by a competent authority.

b. Maintenance of Records. A record of musters and spot-checks are to be maintained for review during security inspections.

c. Accountable Material. Within ACO components all accountable material classified NS, CTS and ATOMAL shall be annually mustered. The report of annual musters of NS material shall be notified to the HQ Security Authority, the report of annual musters of CTS and ATOMAL material shall be reported to the ACO Security Authority through the ACO CACO by the last working day of February (a brief statement confirming the muster/inventory is complete and highlighting any deficiencies noted). In addition, periodic spot checks of Registries and Divisional/personal holdings shall be conducted:

(1) Musters and checks should be coordinated by the HQSO or equivalent and conducted by personnel not concerned with the control or accounting of the material being inspected.

(2) Musters of 25% of CTS and ATOMAL holdings shall be conducted quarterly (for I, II and III quarter only) by ACO component HQ CACO. The results of the quarterly musters of CTS and ATOMAL holdings shall be forwarded to SHAPE SEM J2X through Quarterly Security Returns.

(3) Musters and checks of NS holdings shall be conducted in such a manner as to ensure all holdings are checked at least annually, in addition to the annual muster (for example a check of 10% of holdings on a monthly basis).

(4) Records of the documents mustered on all occasions are to be retained for a period of not less than one year.

(5) For material classified NS and above, up-to-date records of receipt, disposition and dispatch shall be maintained and be subject to periodic spot checks.

Note: The above procedures do not negate the continued requirement for an annual inventory for all holdings classified CTS and ATOMAL.

3-47. **Handover/Transfer Procedures.** Prior to handover/transfer, a muster is to be carried out to ensure that all CTS, ATOMAL and NS documents held on an individual's charge are accounted for. An exception to this rule for NS documents only will be when an individual departs at very short notice. In such cases a full muster of documents classified NS or below held on that individual's charge is to be carried out within three months of departure by a nominated person who is appropriately security cleared.

3-48. **Destruction.** ACO component commanders shall develop and implement a programme for the systematic screening (including downgrading and declassification) and destruction of NATO classified documents, which are no longer required. Surplus NATO classified material including all classified waste such as spoiled papers, amendment residue, working papers, shorthand and other notes, are to be destroyed under supervision in the manners described at Annex K of this directive. It is not necessary to await the originator's approval for destruction of surplus or superseded documents.

a. COSMIC TOP SECRET. CTS and ATOMAL material is normally to be returned for destruction to the HQ Sub-Registry. The destruction is to be carried out under the supervision of the HQ CACO or deputy. ACO component commanders may authorise the destruction of COSMIC material at a Category 1 Control Point. Such destruction is to be carried out by the CCO or his alternate of the Division/Directorate or Agency concerned.

b. NATO SECRET. NS material is to be destroyed by the Document Control Officer under the supervision of an appropriately cleared independent witness.

c. NATO CONFIDENTIAL and NATO RESTRICTED. Destruction of NC and NR material is an individual responsibility.

d. Controlled Working Papers. Destruction of classified working papers which have been brought under control, as provided for in paragraph 3-43, is to be recorded on destruction certificates.

e. Uncontrolled Classified. Classified waste including that resulting from reproduction processes is not to be permitted to accumulate and is to be destroyed in accordance with Annex K; no destruction certificate is required.

f. Exercise Messages. Exercise messages will normally be destroyed upon completion of the exercise. All exercise message logs for CTS and SECRET material are to be affixed to the relevant destruction certificates, which need to contain only sufficient data to identify the material on the attached log. If CTS or NS messages are retained for more than 5 days after completion of an exercise, they are to be brought under formal control.

3-49. **Destruction Certificates.** Destruction of documents classified NS and above is to be recorded on a destruction certificate (reference ACO Form 99). Separate certificates shall be used for each classification. ACO Form 99 is devised to record the full particulars of each document and any locally produced forms are to include all equivalent information.

3-50. In the case of COSMIC documents each destruction certificate is to be signed by the CCO (or, in the case of NS documents, the Document Control Officer) or an alternate, and by an HQ CACO witnessing the destruction.

3-51. Certificates for CTS and ATOMAL documents are to form a permanent record; those for NS are to be retained for 5 years. Destruction certificates may be microfilmed or digitalised. Copies need not be sent to the originator or the dispatching registry, unless specifically requested.

3-52. Destruction certificates are not required for material classified below NS. Classified waste destroyed immediately after the material is produced need not be formally recorded.

3-53. **Emergency Destruction.** All ACO component commanders shall prepare plans for emergency destruction of the most sensitive, and mission- or time-critical NATO classified information. The selected CTS, ATOMAL and CRYPTO material are the first priority for emergency destruction. Individual documents selected for special removal, protection or emergency destruction shall be specially marked. The emergency destruction plans shall be annually reviewed, based on threat assessments.

3-54. **Methods of Destruction.** NCI in hard copy which is no longer required for official purposes, including surplus or superseded information and waste, shall be destroyed in such a manner as to ensure that it cannot be reconstructed. It is the responsibility of each ACO component security authority to approve the destruction process, including methods and products utilised for this purpose. The following minimum requirements shall apply:

a. Shredders:

(1) When shredders are used as a final destruction mechanism for NS and above and special category information, the area of the expelled particle shall not be longer than 5 sq. mm. For information classified NR and NC, the area of expelled particle shall not be larger than 10 mm^2. Shredders shall be cross-cutting in order to enhance confidence that the destroyed information is irretrievable. Shredders are required to have the capacity for manual operation and be constructed so that material cannot be left undestroyed in the machine in operation.

(2) Within ACO components, all shredded CTS and ATOMAL waste shall be additionally incinerated.

(3) When shredders do not meet the requirements of paragraph (1) above within ACO components, there shall be an appropriate onward disposal process where the shredded waste is collected by appropriately security cleared personnel and destroyed using an approved method or process. It is essential that the classified waste shall not be accessible to unauthorised personnel, or be reconstructed.

(4) Any deviation from the requirements described in (1), (2) and (3) above shall be approved on a case-by-case basis by the relevant ACO component security authority, subject to a risk assessment.

b. **Pulpers.** A pulping machine is required to masticate NATO classified waste material by breaking down the fibre resistance. The pulp matter is required to be disintegrated and de-fibred so as to be incapable of reconstruction as recognisable information. A locking device capable of being fastened with double padlocks is required to cover the loading head, or any other aperture providing access to the inside of the tank.

c. **Incinerators.** Shall be constructed to accept sealed bags of classified waste. Any aperture which permits access to classified waste or ash during or after combustion is required to be sealed and padlocked. The ash residue shall be thoroughly destroyed so as not to be readable.

Note: It is the responsibility of personnel witnessing the process of pulping or incineration to ensure that pulp or ash residue is not recognisable once the process has been completed.

3-55. For destruction of removable computer storage media, reference shall be made to the ACO CIS Security Directive AD 070-005.

3-56. It is not necessary to await destruction instructions from the originator for information that is held, but no longer required. ACO component registries that hold such information shall keep it under review to determine whether it is still relevant, or whether it can be destroyed.

CHAPTER 4 – RELEASE OF NATO CLASSIFIED INFORMATION TO NON-NATO ENTITIES

4-1. **Introduction.** Enclosure H to C-M(2002)49-REV1 sets out the policy and minimum standards for the protection of NCI to be released to, or accessed by, non NATO nations and other non-NATO bodies (e.g. International Organisations) including individuals representing such nations or bodies. Furthermore, AC/35-D/1040, the Supporting Document (SD) to NATO Security Policy (NSP) on Information and Intelligence Sharing (I&IS) with non-NATO Entities (NNEs) establishes provisions, mechanisms and procedures to supplement NSP for I&IS with NNEs in order to support Operations, Training, Exercises, Transformation and Cooperation (OTETC) activities at all NATO command levels. I&IS with NNEs shall occur only when the NNE has the need-to-know, balanced by the responsibility to share. For Operations, NATO equipment may also be shared with NNEs, when necessary.

4-2. **General Requirements.** The sharing of NCI with NNEs may take place in the contexts of:

a. NAC-approved cooperative activities where the NNE's participation has been approved by the North Atlantic Council.

b. NATO activities (e.g. programme, project, operation, task) where the NNE's participation and the nature of its engagement in a specific aspect of an activity is deemed beneficial to NATO.

c. Bilateral engagements between a NATO Nation and an NNE, where sharing of NCI with an NNE has been determined to be beneficial to NATO.

4-3. Prior to sharing NCI with an NNE, the NNE and NATO shall have entered into a Security Agreement, the implementation of which shall be certified by the NOS. In the absence of a Security Agreement, a Security Assurance shall be in place where there is a political or operational imperative to share NCI in a timely manner in support of a NAC-approved cooperative activity or, in exceptional cases, outside such an activity. The SD for NATO on Security in Relation to NNEs describes detailed provisions applicable to sharing NCI with NNEs in the contexts specified in paragraph 4-2.

4-4. **Security Agreements and Administrative Arrangements.** A Security Agreement is a mechanism used to enable the exchange of classified information with an identified NNE. It sets out high level strategic principles agreed between NATO and the NNE, providing the basis for the implementation of appropriate security measures to protect NCI as well as the NNE's classified information, when required. The implementation of the Security Agreement by the NNE shall be certified by the NOS before any NCI is released to an NNE.

4-5. The security principles identified in the Security Agreement shall be supported by an appropriate set of Administrative Arrangements. The Administrative Arrangements act in support of the implementation of a Security Agreement and are a set of provisions which outline the basic security requirements for the appropriate and mutually acceptable protection of the exchanged classified information. Once the Administrative Arrangements have been concluded, their application shall be confirmed by the NOS through the conduct of a security survey.

4-6. **Security Assurances.** A Security Assurance is utilised in the absence of a certified Security Agreement between NATO and an NNE, where there is a political or operational imperative that necessitates the sharing of NCI in a timely manner in support of a NAC-approved cooperative activity, or in exceptional cases outside such an activity. The supporting Directive for NATO on Security in Relation to NNEs (AD/35-D/2006) provides detailed criteria to be fulfilled in cases when a Security Assurance is used. A template is provided at Annex M.

4-7. A Security Assurance formalises the NNE's commitment to provide an appropriate degree of protection to any NCI received. A Security Assurance is limited to the specific activity, for a specific period of time. A Security Assurance from an NNE, signed by a representative duly mandated by the NNE, shall be provided to the NOS in cases where a Security Assurance is utilized for the purposes of enabling sharing of NCI in support of a:

a. NAC-approved cooperative activity, or

b. NATO activity, where the NNE's participation has been approved by the NAC or the appropriate delegated authority, on a case-by-case basis.

4-8. **Sponsorship by a NATO Nation.** Sharing of NCI outside activities defined in 12 (a) or (b), further to a special request by a NATO Nation, requires sponsorship. A sponsorship means a form of support provided by a NATO Nation to an NNE in order to enable sharing of NCI with an NNE in case of absence of a certified Security Agreement between NATO and the NNE.

4-9. In order for a NATO Nation to be able to act as a Sponsor, there shall be an appropriate security framework (e.g. security agreement or other applicable arrangement) in place between the Sponsor and the NNE. The Sponsor shall provide a written Security Assurance, signed by a representative duly mandated by the NNE, to the NOS. The Security Assurance stipulates the minimum standards that the NNE shall apply for the protection of NCI.

4-10. A sponsorship is limited to a specific activity, for a specific period of time.

4-11. The SD contains emerging policy covering 7 categories of NNE listed:

a. Contractors (on OTETC activities).

b. Governmental Organisations (GOs).

c. Host Nations (HN).

d. International Organisations (IOs).

e. Non-Governmental Organisations (NGOs).

f. Non-NATO Multinational Forces (NNMF).

g. Non-NATO Nations (NNN) – Including 7NNN[14] and Non-NATO Troop

[14] Refers to the group NNNs with whom NATO has a special relationship: Australia, Austria, Finland, Ireland, New Zealand, Sweden and Switzerland.

Contributing Nations (NNTCN).

4-12. The provisions of AC/35-D/1040 as they apply to ACO/ACT are set out in the Bi-SC Handbook on I&IS with NNEs. Whilst not a Bi-SC Directive, the provisions of the Bi-SC Handbook shall be adhered to. However, when a scenario is not covered within the Bi-SC Handbook, this chapter sets out the policy, principles and procedures required for the release of NCI to, and the exchange of, classified information with non-NATO recipients or international organisations. These arrangements cover information classified up to and including CTS contained in documents issued by the NAC, or by any other NATO committee, command or agency (hereinafter referred to as NATO bodies).

4-13. **Release Authority.** The NAC is the ultimate authority for the release of NCI to non-NATO recipients. This authority adheres to the principle of originator consent and is delegated as follows:

a. The appropriate subject-matter committee for information classified up to and including NS, which has been originated by that committee and/or bodies subordinate to it. For NR, the appropriate subject matter committee may further delegate authority to a clearly identified staff support function or a specific role(s) within the support staffs to that committee.

b. The NATO Military Committee (MC) for information classified up to and including NS, which has been originated by the MC and/or bodies subordinate to it. For NR the MC may further delegate authority to a clearly identified staff support function or a specific role(s) within the support staffs to the MC.

c. SACEUR or DSACEUR for information classified up to and including NS, which is identified as being releasable to xFOR, or is classified NATO/xFOR SECRET (mission SECRET), under the following conditions:

(1) The information is limited to NCI, necessary for the effective participation of non-NATO Troop Contributing Nations (NNTCNs) in operations and exercises, as approved on a case-by-case by the NAC.

(2) The information to be released is only that NCI originating from within ACO and is directly related to specific operations and exercises, where the participation of NNN to that activity has also been endorsed by the NAC on a case-by-case basis.

(3) The ACO Security Authority shall implement an authoritative and auditable process for the release of classified information.

d. The Mission Commander, for an operation involving non-NATO Troop Contributing Nations (TCN), as endorsed by the NAC, for information classified up to and including NS that has already been determined as releasable to the mission (xFOR) under the following conditions:

(1) The information shall be related specifically to the mission.

(2) The information shall be limited to tactical information related to an ongoing operation, and deemed necessary for the successful conduct of the ongoing information.

(3) The Mission Security Authority shall implement an authoritative and auditable process for the release of classified information.

(4) The NOS, in close coordination with SHAPE SEM J2, reserves the right to conduct inspections of the security arrangements in place.

e. The NATO Production and Logistic Organisation (NPLO), for NCI originated by and belonging to one or more of the nations participating in the NPLO.

4-14. The authority for release of NCI shall only be delegated to an appropriate subject matter committee on which the originator(s) is/are represented. If the originator(s) cannot be established, the appropriate subject matter committee shall assume the responsibility of the originator. Authority for release may be delegated to the lowest committee level, best suited to evaluate the importance of the classified information.

4-15. With the exceptions applying to NR information stated in paragraphs 4-4. a., b. above, delegated release authorities cannot further delegate their powers: although, they can entrust subordinate bodies with the implementation of the release decision.

4-16. ACO commands shall keep control of records of information classified CONFIDENTIAL and above, which they have released to non-NATO recipients. These records shall be subject to inspection by the appropriate NATO security authority (e.g. NOS, SHAPE SEM J2).

4-17. **Principles for Authorising the Release of NATO Classified Information.** Authorisation to release shall always be subject to the consent of the originator. The general procedures for such release are at Annex N and the following principles shall apply:

a. For NCI to be released under cooperative activities approved by the NAC, where the non-NATO participants to that activity have been endorsed by the NAC on a case-by-case basis:

(1) Release decisions can either concern clearly identified information or a general category of information.

(2) The subject matter must be included in the general work plan for the activity or in the practical measures established for cooperation.

(3) The release of NCI must be required for initiating cooperation on a specific subject or for the continuance and further development of cooperation within the approved activity.

(4) A Security Agreement, signed by the Secretary General on behalf of NATO and by a representative duly mandated by the non-NATO recipient, must have been conducted. In the absence of a Security Agreement and in exceptional circumstances, in order to support specific operational requirements endorsed by the MC/NAC (e.g. in support of force protection and the exchange of intelligence information), a Security Assurance from the non-NATO recipient, signed by a representative duly mandated by the non-NATO recipient that any information received will be protected in accordance

with its national laws and regulations and to a degree no less stringent than NATO minimum standards, shall have been provided to the NOS.

(5) Where a Security Agreement is in force with an International Organisation, the release of information to its non-NATO members shall be in accordance with the relevant provisions of the Security Agreement, as well as other established rules concerning their participation in NATO activities.

(6) The Security Assurance provided by the non-NATO recipient shall also identify the NATO security classifications and the equivalent security classifications of the non-NATO recipient. The Security Assurance shall be forwarded to the relevant committee responsible for the approval of the release. Copies of the written Security Assurances shall be provided to the NOS who shall maintain a database of Security Assurances.

(7) Only information classified up to and including NC may be released through Security Assurances. However, in exceptional circumstances, in order to support specific operational requirements endorsed by the NAMILCOM/NAC, NS information may be released.

(8) Where there is a requirement to release NS information to a NNN which has signed a Security Agreement/Arrangement with a NATO sponsor, the NATO sponsor shall provide the necessary assurance that the appropriate security system is in place for the protection of such released information, and shall seek the agreement of the relevant committee responsible for the approval of the release prior to its release.

b. For NCI to be released on special request from either NATO member nations; or NATO bodies (the Sponsor) to non-NATO recipients outside of NAC approved cooperative activities:

(1) Release decisions shall be taken on a case-by-case basis and can only concern clearly identified information.

(2) A bilateral Security Agreement/Arrangement shall exist between the NATO member nation sponsoring the release and the non-NATO recipient.

(3) The Sponsor shall be responsible for providing a written Security Assurance, signed by a representative duly mandated by the non-NATO recipient, to NATO from the non-NATO recipient. The Security Assurance provided by the non-NATO recipient shall oblige the non-NATO recipient to protect NCI to a degree no less stringent than the provisions contained in the bilateral Security Agreement/Arrangement for the protection of the Sponsor's classified information. The NATO security classifications shall be identified with their equivalents to the national classifications cited in the bilateral Security Agreement/Arrangement.

(4) The Sponsor shall forward this written Security Assurance to the relevant committee, together with the release request. Copies of written Security Assurances shall also be provided to the NOS.

(5) The request shall demonstrate the advantage which would accrue to NATO. Justifications for release shall be specific, avoiding general statements.

(6) Where a Security Agreement is in force with an international organisation, the release of information to its non-NATO members shall be in accordance with the relevant provisions of the Security Agreement as well as other established rules concerning their participation in NATO activities.

(7) Only information classified up to and including NC may be released through Security Assurances in this case. Where there is a requirement to release NS information to a non-NATO nation which has signed a Security Agreement/Arrangement with a NATO sponsor, the NATO sponsor shall provide the necessary assurance that the appropriate security system is in place for the protection of such released information, and shall seek the agreement of the relevant committee responsible for the approval of the release prior to its release.

4-18. Annex O contains the minimum standards required for the handling and protection of NCI released to and of classified information exchanged with non-NATO recipients. This document will be furnished to all non-NATO recipients with whom NATO concludes a Security Agreement in the context of cooperative activities approved by the NAC.

4-19. **Administrative Arrangements for the Implementation of a Security Agreement.** Administrative Arrangements (AA) necessary for the implementation of the Security Agreement (SAs) have been drawn up and compliance will be confirmed by a security survey of the non-NATO recipient carried out by the NOS. The security survey will establish the ability of the non-NATO recipient to comply with the provisions of the security agreement and with the minimum security standards. The conclusion drawn from the survey will be communicated to relevant NATO bodies.

4-20. **Classification Marking System.** The following procedures shall be used for marking classified information:

a. Existing Classified NATO Information. Classified information that is released to non-NATO recipients will retain its NATO classification. In addition, the cover or first page of any document released and the archived copy will be marked with the name of the release authority, the date the release decision was taken and any related terms or conditions;

b. NATO Classified Information Created within NAC-approved Activities. NCI originated in the context of a NAC approved cooperative activity, shall bear the marking “NATO” followed by the designation of the activity or by the names(s) of the international; organisations or participating nation(s) and the classification level.

NATO and NAME OF ACTIVITY[15] and CLASSIFICATION

[15] NAC approved designator defines community of participants of the specific activity and indicates that NATO information released to such a community will be available to Non-NATO participants of the activity in addition to NATO personnel. Application of NAC approved releasability markings within ACO components is in responsibility of information management cells.

Example:

NATO/EAPC RESTRICTED

c. The originator may restrict access to some non-NATO recipients. In this case a caveat showing the non-NATO recipients who are permitted access shall be added below the classification line.

Example:

NATO/PFP RESTRICTED
AUSTRIA ONLY

d. Classified information created by NATO which is intended to be further disseminated outside the environment within which it was created shall bear the caveat “Releasable to”

Example:

NATO CONFIDENTIAL
Releasable to Sweden

4-21. **Security Arrangements for the Release of NATO Classified Information to Non-NATO Nations, International Organisations and Personnel on Partnership Staff Posts.** NATO security policy sets out the conditions for authorising release of NCI to non-NATO nations and international organisations. Annex P to this chapter outlines the specific security provisions for the exchange of classified information between NATO and the EU.

4-22. **NATO Office of Security Certification.** Upon completion of all administrative arrangements, including a satisfactory security survey of the non-NATO nations’ established security arrangements, the NOS will certify that the non-NATO nation has established security procedures to safeguard NCI. Information regarding the nations possessing a NOS-certified Security Agreement be found on NOS’ “Roadmap to NATO Security Related Policies, Supporting Directives, Supporting Documents, and Guidance Documents” webpage (https://hqhome.hq.nato.int/nos/Security%20Policy/NOS%20Roadmap/Startpage.pdf) or can be sought at SHAPE SEM J2X SPO. It must be noted that NOS certification does not constitute authority to release NCI; the procedures for release to NNN and international organisations identified at Paragraph 4-8, shall be followed.

4-23. **Access to NATO Classified Information by Partner Officers on Partnership Staff Posts.** Partnership Staff Posts (PSP) personnel are an integral part of the NATO staffs where they are employed and NATO and local ACO security policies and regulations apply to them:

a. Necessary security controls are to be implemented as appropriate by the local ACO commanders as Risk Owners, in accordance with NATO security policies and with the approval of SHAPE ACOS SEM J2 as the ACO Security Authority. Both physical access and access to classified information by PSP personnel will be governed by these policies and regulations, including the need-to-know principle. Access authorisation, including unique passes, must be in line with security policies.

b. The same NATO Security Policy governs all NATO staffs, however, where required ACO Commanders hosting PSP personnel may have their own additional unique requirements and specificities regarding information management and security regulations. Specific security requirements shall be developed by the respective sponsoring ACO element for the respective Job Descriptions and submitted to the ACO Security Authority for approval.

c. To enable access to NCI to an individual from a Partner Nation filling a PSP position, in accordance with NATO Security Policy and its supporting directives, the originator's consent is normally required. However, when the allocation of a PSP position to a specific Partner Nation implies there could be an exception to the requirement for originator control, a decision by the National Security Authorities through the Security Committee's approval shall be sought.

d. All PSP personnel require some level of access to a CIS, which offers electronic connectivity to the offices and staff with whom the PSP will be working. However, Partner officers may not necessarily have electronic connectivity to NATO classified networks. NATO staff may need to share relevant information with PSP personnel in fulfilment of their day-to-day responsibilities across PSP enabled NATO CIS.

e. ACO command structure elements hosting PSP personnel are required to determine the information needs of PSP personnel in order to develop more efficient and practical functional working relationships. These information needs should be reflected in the Job Description.

4-24. **Records of Released Information.** NATO Civil and Military bodies shall keep records of decisions of all information classified NC and above which they have released to an NNE and shall, at least every six months, report details of the reference number, title and release date to the NATO Central Registry, Brussels, unless otherwise directed by an appropriate Security Authority.

PART IV

PERSONNEL SECURITY

CHAPTER 1: Access to NATO Classified Information

CHAPTER 2: Security Education and Awareness

CHAPTER 3: Travel Security

This page is intentionally left blank.

CHAPTER 1 – ACCESS TO NATO CLASSIFIED INFORMATION

1-1. **Introduction.** This chapter of the ACO Security Directive refers to Enclosure C to C-M(2002)49-REV1 Security within NATO, and to the Directive on Personnel Security AC/35-D/2000-REV8, dated 25 November 2020. This chapter contains mandatory provisions regarding personnel security within ACO and also information which clarifies the meaning of those provisions.

This chapter addresses the following aspects:

a. Personnel Security Clearances (PSCs);

b. Responsibilities with respect to personnel security;

c. Standards and procedures for a renewal of a PSC;

d. Standards and procedures for addressing adverse information about an individual holding a PSC;

e. Records and means of confirmation as to whether an individual is in possession of an appropriate PSC;

f. Access to NCI in exceptional circumstances; and

g. Access to NCI by Integrated Members employed by an ACO component headquarter.

1-2. **Personnel Security Clearance (PSC).** In accordance with the requirements of NATO Security Policy, there are agreed standards of confidence about the loyalty, trustworthiness, and reliability of all individuals granted access to, or whose duties or functions may afford, access to NATO information classified NATO CONFIDENTIAL (NC) and above. In order to achieve this, individuals who require access or may have access to information classified NC and above during the course of their duties shall have a PSC, at the appropriate level, which is valid for the duration of the authorised access. In addition, such individuals are required to:

a. Have a need-to-know.

b. Have been briefed on their security obligations in respect to the protection of NCI.

c. Have acknowledged their responsibilities in writing, which ensures non-repudiation.

1-3. A PSC will be based on a security investigation process that is in full compliance with NATO Security Policy, along with confirmation from the appropriate National Security Authority (NSA) / Designated Security Authority (DSA) that the individual in question may be authorised to access NCI.

1-4. A PSC is not required for access to information classified NATO RESTRICTED (NR). Individuals who only require access to information classified NR shall be briefed on their security obligations and shall only be afforded such access on a need-to-know basis.

1-5. When a PSC is granted, it shall be valid for a period not exceeding 10 years for information classified NC and NS, and not exceeding 7 years for COSMIC TOP SECRET (CTS).

1-6. **Personnel Security Clearance Confirmation (PSCC).** In situations where an individual will attend or participate in an activity requiring access to NCI at the level NC and above (e.g. conference, meeting, course, seminar), a confirmation of the existence of a PSC is required.

1-7. Confirmation of existence of an individual's PSC shall be communicated through official channels (e.g. NSA/DSA to ACO component HQ through NMR or HR office) and shall only be hand-carried by the concerned individual in exceptional circumstances. A template for a PSCC request is provided at Annex Q. ACO component HQSOs shall confirm the existence of an individual's PSC by one of the following methods:

a. PSCC, a template of which is provided in Annex R.

b. Request for Visit (RFV), a template of which is provided in Tab 2 to Appendix 1 to Annex S.

c. Exceptionally, when timely confirmation of an individuals' PSC is of paramount importance for the execution of a mission, by other means communicated directly between the NSA/DSA and the ACO component HQSO.

1-8. If an individual's PSC is revoked, suspended or altered (e.g. change in validity or level), the responsible NATO Nation and/or ACO component HQSO shall inform all the recipients of that individual's PSCC of the change.

1-9. PSCCs for individuals working at ACO component HQs. The existence of an individual's PSC shall be confirmed when an individual is to be employed by, or seconded to, an ACO component HQ, or assigned by a NATO Nation to its national representation at an ACO component HQ. This is accomplished by one of the following methods:

a. Upon specific request by the ACO component HQ, by using the Request for PSCC template (Annex Q).

b. Directly by the NSA/DSA (by using the template at Annex R).

1-10. An individual's parent NSA/DSA shall be requested to provide confirmation that their PSC remains valid if:

a. An individual's period of employment does not commence within 12 months of the issue of a new PSC to fill the post within an ACO component HQ;

b. There is a break of 12 months in an individual's employment, during which time the individual is not employed in a post within an ACO component HQ, NATO Nation's government, or other NATO civil or military body.

1-11. **Responsibilities.** NSAs/DSAs are responsible for:

a. Carrying out security investigations on their nationals and other persons within their jurisdiction, who require access to information classified NC or above,

and determining whether a PSC should be granted, denied or revoked, following the principles of NATO Security Policy.

b. Ensuring that PSC procedures are carried out with the knowledge and consent of the individual being investigated.

c. Renewing PSCs and verifying their existence.

d. Informing the recipients of a PSC Confirmation in cases of revocation, suspension or any alternation to a PSC.

e. Cooperating with other NSAs/DSAs in carrying out their respective procedures.

1-12. ACO component HQs are responsible for:

a. Identifying those posts which require a PSC (by HQ J1 Personnel and/or HR cells in coordination with Divisional Security Officers (DSOs)).

b. Based on the need-to-know principle, authorising access to NCI within their area of responsibility (by HQSOs or DSOs, following the ACO Form 107).

c. Ensuring that personnel security standards within subordinated HQs, as set forth herein, are met (accordingly by SHAPE J2X J2/G2/A2/M2 security and CIS security policy SMEs).

d. Evaluating the continuing eligibility of their staff for access to NCI, especially to information classified CTS and special category (by DSOs and HQ CACOs).

e. Informing the relevant NSA/DSA when an individual no longer requires a PSC and/or access to NCI (by HQ's Personnel and/or HR cells in cooperation with DSOs).

f. Supporting NSAs/DSAs through the provision of relevant information to assist the security clearance process (by HQ J1, Personnel and/or HR cells in coordination with HQSO and DSOs.

g. Reporting actual or potential security concerns regarding an individual holding a PSC to the respective HQSO, as well as with principles outlined in Part VI of this Directive.

1-13. ACO component HQSOs shall monitor the PSC validity for each assigned member of staff and apply for its renewal at least 12 months prior to the expiration date of the valid PSC.

1-14. For renewal of PSCs, the procedures outlined below shall, as a minimum, be carried out:

a. The completion of a personnel security questionnaire by the individual concerned (form shall be supplied by the supporting NSA/DSA).

b. For individuals employed by an ACO component HQ, a check of the personnel security questionnaire against the security and personnel records is to be

conducted by the HR team in coordination with HQSO.

c. When a renewal is requested by an ACO component HQ for individuals employed by the HQ, the completed personnel security questionnaire in (a) above and results of the check in (b) above shall be sent by the HQ HR team to the individual's parent NSA/DSA.

d. When the relevant ACO component HQ requests the individual's parent NSA/DSA to renew the PSC, it shall also provide details of the individual's security record (copy of ACO Form 107) for the period of employment under review.

1-15. Exceptionally, if a PSC is not renewed before its expiration date, the J1 Personnel or **HR cell of the ACO component HQ employing the individual shall:**

a. Request from the individual's parent NSA/DSA an extension of the current PSC, if permitted under national law and regulations; and

b. Request from the individual's parent NSA/DSA an interim or temporary PSC, if permitted under national law and regulations; or

c. The ACO component HQ Security Authority may grant continued access to NCI provided that:

(1) The individual's parent NSA/DSA has confirmed that the clearance renewal procedure is still ongoing;

(2) The ACO component HQ is willing to accept the risk with the individual's continued access to NCI; and

(3) The decision to grant access to NCI is reviewed and confirmed by the HQ Security Authority every 6 months until the PSC is renewed.

1-16. Changes to an individual's PSC. When an ACO component HQ receives the decision of a parent NSA/DSA that a PSC is suspended or revoked, the relevant HQSO shall immediately exclude the individual from access to NCI. In addition, the individual shall be made aware of their continuing responsibility to protect NCI they had access to and advised of the consequences of failing to do so. An acknowledgement in writing (ACO Form 107) should be used for such debriefing.

1-17. **Security Briefings.** All members of staff employed in posts where they have access to NCI shall be briefed on security procedures and their security obligations in respect to the protection of NCI. Individuals shall acknowledge in writing that they fully understand their responsibilities and the possible consequences to them, outlined in their national law and regulations if they are found to have allowed NCI to pass into unauthorised hands, either by deliberate intent or through negligence. A record of the acknowledgement (ACO Form 107) shall be maintained either by ACO component HQSO or DSOs, and kept by the HQSO accordingly for NC and NS up to 5 years, and for CTS up to 10 years.

1-18. When conducting briefings security staff should make full use of ACCI personnel if available to present Terrorism, Espionage, Sabotage and Subversion (TESS) threat awareness information.

1-19. **Initial Briefings.** Prior to initial access to NCI, all personnel are to be briefed on NATO security procedures and of the consequences of negligence. Special emphasis is to be placed on the need for stringent control of CTS information.

1-20. **Periodic Briefings.** In addition to the initial brief, it is important that personnel who are required to handle NCI are periodically reminded of the dangers to security arising from indiscreet conversation with persons having no 'need to know'; their relationship with the press, and, the threat presented by the activities of hostile intelligence services which target the Alliance and the constituent member nations. Such persons are to be thoroughly briefed on these dangers and the reporting procedures should they be the subject of a possible security incident. Briefings are to be conducted annually. Records of such briefs are to be recorded on ACO Form 107.

1-21. **ATOMAL Briefings.** All personnel are to be briefed in accordance with Annex T prior to access to ATOMAL information and annually thereafter. Briefs are to be recorded on ACO Form 107.

1-22. **Departure De-Briefings.** On departure from an ACO organisation, individuals are to be de-briefed on their continuing responsibility to safeguard information gained through employment in the NATO organisation. The ACO Form 107 is to be annotated accordingly.

1-23. After an individual's departure or termination of employment/contract within an ACO component HQ, their personal security file(s), including Forms 107, shall be retained for investigative purposes respectively for:

a. 5 years for personnel granted access to NATO SECRET information.

b. 10 years for personnel granted access to COSMIC TOP SECRET information.

1-24. **Interim or Temporary PSC.** In instances where either the initial clearance process has been commenced, but not yet completed, or an individual's PSC is being renewed, when the parent NSA/DSA has determined that the individual presents no risk, their continued access to NCI may be granted based on an Interim or Temporary PSC, issued in accordance with national laws and regulations. It is the ACO component HQSOs responsibility to ensure the relevant parent NSA/DSA is aware that the individual has:

a. A continued 'need-to-know'.

b. Been briefed on their security obligations in respect to the protection of NCI.

c. Formally acknowledged their responsibilities in writing.

1-25. **Provisional Appointments.** When an individual is assigned within an ACO component HQ to a post, or has been nominated to a secondary function (e.g. HQ CACO, CCO), that requires a PSC at a level higher than that currently held, the HQ Security Authority may provide exceptional, but provisional approval; however, the following requirements shall be met:

a. The individual is to possess a current PSC.

b. The security clearance process for obtaining the level of PSC required for the post or function has been initiated.

c. Satisfactory checks have been made by the HQSO to ensure the individual has not seriously or repeatedly infringed security regulations.

1-26. The record of individuals that have been granted access based on temporary clearances and/or provisional appointments shall be maintained by the ACO component HQSO and forwarded quarterly via QSRs to SHAPE J2X SPO. The HQSO shall also immediately inform the parent NSA/DSA on granting such access to the individual.

1-27. **Administration of PSCs.** Each ACO component HQ is to maintain a central record of their NATO PSCs and an individual security record for each assigned member of staff. ACO Form 107 is to be used for this purpose. A specimen ACO Form 107 is at Part VIII, but the format may be expanded to suit local circumstances. When military or civilian personnel are transferring to another posting within ACO, the HQSO is to forward the PSC to the new organisation.

1-28. Each ACO component HQ shall also maintain a dedicated central record of non-NATO individuals granted unescorted access to a NATO Security Area.

1-29. Personnel who arrive to take up appointment without the requisite confirmation of PSC are to be assumed to be uncleared. They may be permitted escorted access to designated NATO Security Areas, but shall not be provided with access to any NCI higher than NR.

1-30. Civilian employees or prospective employees are not, in any instance, to be advised that employment is offered subject to security clearance. Moreover, in cases of discharge or re-assignment of civilian personnel, security considerations are never to be cited to the individual as the basis for the action without the explicit prior approval of the relevant parent NSA.

1-31. **Access to NATO Classified Information.** Each individual in possession of NCI is responsible for ensuring that persons to whom it is passed are authorised to have access to information of at least that specific classification. The responsibility for authorising access to NCI and for briefing of personnel on NATO security procedures rests with the commander of each ACO component HQ.

1-32. ACO component HQs that sponsor delegates to classified conferences and meetings away from their parent organisation, are to transmit a PSCC to the appropriate authorities that such delegates are authorised to have access to NCI of the appropriate level. The format for this notification is at Annex R. Where persons make repeated visits, the Security Officers of each organisation may make appropriate arrangements; however, these arrangements should not be open-ended and should have review dates based on need and PSC expiry dates.

1-33. **Access to COSMIC TOP SECRET Information.** Access to CTS information must be specially controlled. A Security Authority of each ACO component HQ will specifically authorise those who are required to have such access. Persons who are authorised access will be recorded in the appropriate ACO CTS/A Central Registry, HQ CTS/A Sub-Registry, or Control Point. The names of all persons ceasing to be employed in duties requiring access to CTS information are to be removed immediately from the CTS access

list. The CTS access list shall be dated and signed. It shall also include the Rank, Name, clearance level and expiration date of the PSC of the personnel who are authorised.

1-34. **Access to ATOMAL Information.** Access to ATOMAL information must be specially controlled. A Security Authority of each ACO component HQ will specifically authorise those who are required to have such access. Persons who are authorised access will be recorded in the appropriate ACO CTS/A Central Registry, HQ CTS/A Sub-Registry, or Control Point. The names of all persons ceasing to be employed in duties requiring access to ATOMAL information are to be removed immediately from the ATOMAL access list. The ATOMAL access list shall be dated and signed. It shall also include the Rank, Name, clearance level and expiration date of the PSC of the personnel who are authorised.

1-35. **Access to NATO Crypto Information.** NATO PSCs are equally applicable for eligibility to receive access to NATO crypto information. Additionally, individuals who are required to have access to high grade NATO keying material must be specifically authorised by the commander of the ACO component HQ, in accordance with the procedures set forth in NATO crypto security instructions which have been promulgated by the NATO Military Committee.

1-36. **Temporary Access.** Exceptionally, individuals employed within an ACO component HQ may be authorised, on a one-time basis, access to NATO information classified higher than their current PSC. In order to be granted this access, the following criteria must be fulfilled:

a. A compelling mission need for the access shall be justified, in writing, by the individual's supervisor.

b. Access shall be limited to specific items of NCI in support of the mission described by the supervisor.

c. Satisfactory checks have been made by the HQSO that the individual has no serious or repeated infringement of security regulations.

d. Authorisation shall be granted by an HQ Security Authority to at least OF6 level.

e. A record of the exception, including a description of the information to which access was authorised, shall be maintained by the HQSO.

f. Details of the exception, including a description of the information to which temporary access was authorised, shall be forwarded by the HQSO quarterly via QSRs to SHAPE J2X SPO.

1-37. This procedure shall not be used on a recurring basis for access to NCI. If this is required, or if access is required for more than 6 months, a PSC for the higher level shall be obtained and the PSC requirements of the post updated.

1-38. **Senior Government Officials.** Access to NCI by Senior Government Officials (SGOs) (e.g. Heads of State and Government, Government Ministers, Members of Parliament, and members of the Judiciary) is determined by the national laws and regulations; such SGOs shall be briefed on their security obligations and shall have a

need-to-know. The SGO parent NSA/DSA can be consulted if there is a need to determine whether an SGO can be granted access to NCI without a PSC.

1-39. **Contractor Personnel.** The provisions for PSCs or confirmation of those for contractor personnel performing work on NATO premises and requiring a PSC is addressed in Part VII of this Directive.

1-40. **Interpreters.** Exceptionally, access to NCI for the purpose of translation or interpretation by translators either from NATO or non-NATO nations who do not have an appropriate PSC for the purpose of translation or interpretation is permitted, taking cognisance of the following:

a. The language to be interpreted requires a mother tongue speaker and makes the individual essential/critical with respect to the activity.

b. Access shall be authorised by the HQ Security Authority, based on compelling written justification.

c. Access shall be limited to specific items of NCI up to and including CTS in support of the mission described by the HQ Security Authority.

d. Access to CIS processing NCI shall not be authorised, other than to CIS intended solely to support the activity (Mission Network) in which the individual is engaged.

e. Record of decisions on exceptional access to NCI by interpreters without a PSC shall be maintained by the HQSO and shall be forwarded quarterly via QSRs to SHAPE J2X SPO.

f. Information on decisions taken within ACO on exceptional access to NCI by interpreters without a PSC shall be forwarded by SHAPE J2X SPO to the NOS bi-annually on 30 January and 30 June.

g. Individuals without a PSC who have been granted access to NCI for interpretation, have been briefed on the relevant security procedures and have acknowledged in writing that they fully understand their responsibilities and the potential consequences should there be unauthorised disclosure, either by deliberate intent or through negligence.

1-41. **Emergency Access.** In wartime, during periods of mounting international tension, international contingency operations or in peacetime when emergency measures require it, an ACO component HQ Security Authority may, in exceptional circumstances, grant by written authorisation, access to NCI to individuals who do not possess the required PSC, provided that such authorisation is absolutely necessary and there are no reasonable doubts as to the loyalty, trustworthiness and reliability of the individual concerned. A record of this authorisation describing the information to which access was granted, shall be maintained by the HQSO. Details of the emergency access, including a description of the information to which access was granted, shall be forwarded by the HQSO quarterly via QSRs to SHAPE J2X SPO.

1-42. In the case of information classified CTS, this emergency access shall be confined whenever it is possible to those individuals who have been authorised access to either national TOP SECRET or to information classified NS.

1-43. **Access to NCI by Integrated Members.** Members of non-NATO nations are considered to be Integrated Members of either a NATO Nation's civil or military body when they are fully incorporated into that body as constituent members therein and are treated by that body as being equal in every manner, where their PSCC (template provided at Annex U) is either provided by their parent nation or the NATO Nation with the same legal obligations as a NATO national.

1-44. Integrated Members of a NATO Nations civil or military body may be authorised access to NCI provided such access is necessary in support of a specified, ACO component led NATO operation, mission, activity or program. Prior to providing access to NCI, the respective ACO component HQSO shall confirm that the following conditions are met:

a. The NATO Nation is willing to share its own national classified information of a similar type and classification level with a non-NATO nation of which the Integrated Member is a citizen.

b. The individual in question has been granted a PSC based on a clearance process no less rigorous than that required for a NATO national in accordance with the NATO Security Policy.

c. The NATO Nation has sufficient control and jurisdiction over the individual in order to take appropriate legal action and hold them accountable for improper handling of NCI.

d. Access is not provided to ATOMAL or other Special Category Information.

1-45. All other cases where individuals representing Non-NATO Entities require access to NCI are detailed in the Bi-SC Handbook on Information and Intelligence Sharing with Non-NATO Entities.

1-46. **Insider Threat.** The Insider Threat is represented by personnel who have privileged access to NCI and/or assets by virtue of their role within the ACO component HQ and could subsequently abuse this access to destroy, damage, remove or disclose NCI and/or NATO assets either by deliberate intent or negligence.

1-47. While responsibility for assessing the individual's eligibility for a PSC rests with the parent NSA/DSA, the ongoing awareness with regard to the protection of NCI is the responsibility of the ACO component HQ employing the individual in the context of countering the risk of Insider Threat. The employing ACO component HQSO shall report relevant security concerns about the employed individual having a PSC to the NSA/DSA that issued the individual's PSC, in order to determine whether the individual shall continue to hold a PSC.

1-48. In addition, a layered approach of security countermeasures should be in place to mitigate the risk of the Insider Threat. Such countermeasures should encompass:

a. Effective security line management allowing for identifying and addressing behaviour with potential security implications (within ACO component HQs security line management encompasses the HQSO, DSOs, BSOs, DCOs, CIS Coordinators, CACOs, CCOs and CRYPTO Custodian appointments, and ACCI).

b. Good general management practices which increase employees' commitment and loyalty.

c. Performance evaluation processes that include addressing any security issues related to the specific individual, post or organisation.

d. Robust, based on determined need-to-know, access control to specific Security Areas and CIS, to identify any unauthorised activity.

e. Mandatory reporting of changes in an individual's personal circumstances for those personnel holding a PSC; particularly those with a PSC at the CTS level, holding sensitive posts (e.g. related to NUCOPS, SIGINT, CRYPTO, CTS/A Registry).

f. Regular, managed by the HQSO, security awareness training and establishment of a security culture, enforcing strong compliance with security procedures (requirements for security awareness and education within ACO component HQs are detailed in Chapter 2).

1-49. **Reporting Adverse Personnel Matters.** If an ACO commander becomes aware of any adverse factor, which might affect the security reliability of an individual, the parent NSA/DSA is to be informed through the appropriate channels. Similarly, each member nation is responsible for informing the security authority of the ACO component HQs of adverse factors, which might affect the security reliability of an individual.

1-50. **Removal of Personnel from Post.** Any person considered to represent a risk to NATO is to be removed from positions and situations where they might endanger security, pending the final decision as to further employment within ACO. In the event of withdrawal of clearance, the parent NSA/DSA will inform the relevant ACO commander whether the person may be told that his PSC has been withdrawn. Thereafter, the matter is entirely the responsibility of the parent nation.

This page is intentionally left blank.

CHAPTER 2 – SECURITY EDUCATION AND AWARENESS

2-1. **General Principles.** All personnel assigned to ACO are to be made aware of security risks and threats in order to support the development of an appropriate security attitude in individuals and improve the overall security culture within the Organisation and its related security posture. ACO commanders shall ensure appropriate security education and awareness programmes are conducted. Personnel are to be made aware of the threats to security and also the minimum standards to which they are to adhere.

2-2. **Knowledge of Security Instructions.** Supplements to this directive and other locally-created security instructions shall be available to all HQ personnel on headquarters' NS and/or UNCLASSIFIED networks in a form in which they can be easily consulted and understood. In HQs with substantial security concerns and/or responsibilities, local security instructions may be long and detailed. In such HQs, it is unlikely that an individual staff member will, or needs to, know every single stated regulation; however, each staff member should be provided with, or have access to, a concise version that:

a. Describes the principles of good security behaviour, both at and outside the HQ.

b. Lists the fundamental security procedures that shall be followed by every staff member.

c. Draws attention to the HQ's local security instructions, states where they are available, and emphasises that ignorance of their contents is not an excuse for failure to comply with the security instructions.

2-3. **Security Awareness Officers.** A Security Awareness Officer, normally the HQSO, shall be appointed to develop and oversee a comprehensive Security Education and Awareness Programme, including the regular provision of security education and the maintenance of security awareness throughout the HQ. Security Awareness Officers shall have a thorough knowledge of NATO Security Policy and local security regulations, and be in a position to answer questions, or at least identify the responsible person/office within the organisation who can answer the questions. The Security Awareness Officer should have the ability to motivate staff members with respect to security as personnel may have to be convinced to understand that the security provisions are sensible and important to them and to the entire organisation.

2-4. **Responsibilities.** SHAPE SEM J2X SPO personnel will supervise and support security education and awareness activities within ACO in order that ACO HQs can enhance their individual security education and awareness programmes. ACO Security Awareness Officers are responsible for planning and conducting security education and awareness activities within their HQ to ensure that all personnel receive security instruction upon employment and at regular intervals, on the need for security and the procedures for achieving it.

2-5. **Objectives of Security Education and Awareness.** When developing a security education and awareness programme, the objectives should be clearly identified, such as:

a. To ensure that members of HQ staff are aware of the threat from terrorism, espionage, intelligence services, subversion or sabotage (TESS).

b. To educate HQ personnel in the general requirements of protective security, covering physical security, security of information, security procedures and CIS security. It is essential that security not only make sense, but is seen to make sense also.

c. To ensure that HQ personnel remember the need for security and follow the security requirements of their HQ. This is accomplished through a programme of re-briefings and security reminders and by making security an issue in job evaluation discussions.

Introducing personnel to the need for security will not ensure that they remain security-minded as security requirements are only one aspect of a person's job function and priority will soon be given to other considerations. Consequently, there is a need for security reminders, bringing home the importance of security in its own right in relation to the day-to-day requirements of the office environment. Personnel should also be reminded of good security practices during out-of-office hours.

2-6. **Methods of Security Education and Awareness**

a. Lectures, Seminars and Workshops. Lectures, seminars and workshops are the usual medium for security awareness. They can be broadly divided into two groups:

(1) Information about the threats from terrorism, espionage, intelligence services, subversion or sabotage. This information should be provided by subject matter experts with first-hand experience of the subject, who can amplify their information with examples and case histories.

(2) Information about protective security. This information should be given by HQSOs and/or subject matter experts with specific security responsibilities (i.e. in the area of CIS and cyber security). The information provided should be related to regulations coming from this directive and from local security instructions to which the members of staff are required to comply. The information provided should encourage questions and discussions in order to:

(a) Clarify any misunderstandings that may exist about this directive and/or the local security instructions.

(b) Clarify the importance of security requirements with respect to meeting operational or administrative requirements.

(c) Highlight the consequences of security violations.

b. Informal Talks to Small Groups. Informal talks may be useful in order to meet a particular purpose, for example:

(1) When introducing HQ personnel to the security requirements of a specific task (e.g. an operation or mission).

(2) To address specific security concerns and/or problems.

(3) As an effective follow-up to lectures, seminars and workshops.

(4) Dealing with a specific aspect of security.

(5) As a means of obtaining HQ personnel participation in the formulation of a security education and awareness programme.

c. Individual Briefings. Individual briefings should be given when an individual is preparing for a particular activity for which a specific briefing is required, such as travel to countries with specific security risks, or acting as a courier for classified material. Individual briefings can be of special value in certain cases, for example:

(1) When a staff member is first assigned to duties involving access to NCI or to duties where special security measures are in force.

(2) When an individual has been determined responsible for, or has been involved in, an actual or potential breach of security.

(3) When there are indications that an individual's attitude towards protective security is poor or does not meet NATO standards.

d. Visual Aids. Visual aids are of value in demonstrating a particular point made in a lecture or talk and should also add interest and/or clarity to the subject matter. Examples of visual aids include not only computer-based presentations but also demonstrations of security equipment, products or mechanisms.

e. Computer-Based Trainings (CBTs). CBT directly involves the recipient in the process of security education, explains basic principles and minimum standards of NATO security policy, and should be followed by some method of assessing the trainee's subject knowledge (e.g. a multiple choice questionnaire). CBTs offer the advantage of standardized training across multiple audiences and/or iterations as well as reducing subject matter expert manpower and increasing scheduling flexibility. CBTs are most applicable to initial and periodic training; however, they may also be applicable as a condition for reinstatement of suspended access following a breach of security.

f. Video Productions. Video Productions are a useful means of security education provided that their instructional value takes precedence over entertainment value. Videos should not be too long, should be focused and may include some degree of entertainment in order that the attention span of the target audience is maintained. A discussion on the objectives to be learned should follow the showing of the film. Any discussion is given added impetus if the discussion uses the subject of the video to focus on specific local security instructions.

g. All User Messages (AUMs). AUMs can be effective security reminders when employed thoughtfully. They may best make an impression if they are directly related to a security breach and its consequences within the organisation. AUMs should not be sent out to personnel on a regular and regimented basis; rather, they should be sent out at random intervals to avoid the "delete without reading" syndrome.

h. Posters. The impact of security posters tends to be short lived; they may become "part of the furniture". To ensure that posters have an effect, they need to

be eye- catching, changed frequently and put up in positions where they are likely to have the greatest impact.

i. Competitions and Contests. Competitions with prizes can be an incentive for individuals to provide new ideas for security awareness. This can lead to increased thinking about, and discussion of, security rules and practices.

j. Warning Notices. Warning notices should be used on:

(1) Telephones – to warn that speech on the telephone is not secure.

(2) Office doors/walls – to remind personnel to ensure that all classified documents (including removable computer storage media) are secure prior to leaving the office for a particular period of time.

(3) Security containers – to remind personnel to ensure that the security container is locked or the combination is appropriately scrambled before the office space is vacated.

(4) Computers – to remind users of the highest classification level of information that can be stored, processed and/or transmitted.

2-7. **Security Awareness Programme Content.** While the previous points identify the objectives and methods of security awareness, a security awareness programme coordinates these aspects in order that individuals are informed about the importance of security, both at the beginning of their duties and also subject to periodic reminders. As a minimum, the key topics listed in Annex V shall be covered.

2-8. **Newcomer Activities.** As part of the introduction to the HQ, all newcomers shall be provided with access to, and directed to read and understand, this directive, the local security instructions and the CIS SecOPs. Additionally, the Security Office shall provide a security briefing to the individual covering, as a minimum, all of the topics listed above. Following the briefing, the newcomer shall sign ACO Form 107 as acknowledgement of his responsibilities associated with the protection of NCI. If the security briefing is provided, in full or in part, by CBT, the newcomer shall provide certificates of completion prior to receiving access to NCI.

2-9. **Continuous Security Education and Awareness.** Periodic security refresher training shall be provided to all personnel with access to NCI annually, at a minimum. In addition to covering all of the topics listed above, periodic refresher training should include topical security matters relating to, for example, security incidents or breaches that have occurred within the HQ. Staff members may be invited to re-sign the ACO Form 107 following refresher training. Additionally, prior to departure from post, the individual should be debriefed by the Security Office on the continuing responsibilities associated with NCI and sign the ACO Form 107 as acknowledgement of those responsibilities.

2-10. **Breaches of Security.** Breaches of security may indicate a need for remedial action, such as amendments to existing local security instructions, additional security education (e.g. CBTs), and/or disciplinary action. Every opportunity shall be taken to use breaches of security as a means of providing security education to the individual concerned. In addition to the periodic refresher trainings, the Security Awareness Officer shall ensure that individuals who have breached security receive remedial security training

and obtain CBT certificates (if applicable) to restore suspended access. Where an individual is a repeat offender, the Security Office may escalate the process and involve HQ senior management in reinforcing the individual's security obligations.

2-11. **Quarterly Security Returns.** The Quarterly Security Returns (QSRs) assist the ACO Security Authority to maintain oversight across the ACO Command Structure and to improve the ACO Command Group's situational awareness on security issues. Additionally, policy deficiencies and examples of best practices derived from analysis of the QSRs will be used as a base for developing ACO-wide security education and awareness training. ACO commands shall submit QSRs to SHAPE SEM J2X SPO on a quarterly basis (April, July, October, and January). Required reporting format is at Annex W.

2-12. **Training of Security Officials.** The NATO School in Oberammergau (Germany) provides a NATO Security course twice per year for personnel assigned to designated security positions. SHAPE SEM J2X provides a security course for ACO security personnel, including those in collateral security positions (e.g. DSO, BSO) once per year. The aim of these two courses is to familiarise ACO personnel involved in security with the requirements of NATO security policy and ACO-specific security regulations coming from this directive. Taking into consideration the importance of improving unity of doctrine regarding the security protection of information, the HQSOs shall periodically organise appropriate security awareness training for Command Group personnel and security officials, including collateral security staff.

This page is intentionally left blank.

CHAPTER 3 – TRAVEL SECURITY

3-1. **Temporary Duty Travel.** It is understood that modern ways of working and the disparate nature of ACO means that Temporary Duty Travel (TDY) is common place. Furthermore, it is understood that many personnel who work for ACO will need to travel to countries that are not NATO members. In these circumstances, it is essential that personnel who do travel as a part of their official duties are fully aware of the threats ranged against them. Personnel shall contact ACCI prior to and when they return from TDY, should they be going to a country that is not a NATO Member Nation. Personnel should make ACCI aware of their travel plans to include:

a. Where they are travelling to.

b. Their dates of travel.

c. Who they are travelling with.

d. Reason for travelling.

e. Rough outline of their itinerary.

f. What personal and NATO Personal Electronic Devices (PED) and/or laptops they will be taking with them.

3-2. Personnel returning from TDY from a Non-NATO country shall contact ACCI if they feel that they have been subject to any form of unusual activity or they feel that they have been the target of Hostile Intelligence Service (HIS). It is imperative that ACO personnel remain vigilant and understand that they may well be the target of Hostile Intelligence Services.

3-3. **Private Travel.** ACO personnel should also be aware of threats to themselves and their families when they are on private travels. Personnel should consult their National Travel Advice websites prior to booking any holidays, especially when travelling outside of NATO Nations. Equally, ACO personnel should be aware that they may be targeted by HIS, Organised Crime or opportunist crime when they are abroad and should act accordingly.

This page is intentionally left blank.

PART V

COMMUNICATION AND INFORMATION SYSTEM SECURITY

This Part has been removed to separate ACO Directive AD 070-005.

This page is intentionally left blank.

PART VI

SECURITY PROCEDURES

CHAPTER 1: Security Incidents

CHAPTER 2: Security Inspections

This page is intentionally left blank.

CHAPTER 1 – SECURITY INCIDENTS

1-1. **General.** The protection of NATO personnel, assets, operations and programmes is dependent upon the effective implementation of appropriate security measures and policy by personnel who are suitably trained and are aware of the threat, their responsibilities and properly supervised. Commanders, and indeed personnel, need to appreciate that good security awareness, practices and measures are backed up by administrative, disciplinary, and in the extreme cases, legal sanctions.

1-2. **CIS Security Breaches.** Due to the nature and proliferation of Communications and Information Services (CIS) and the speed with which breaches of security can affect other CIS, it is necessary to enhance the reporting and investigating procedures detailed in this Chapter. Therefore CIS related security incidents shall be handled and reported in accordance with the respective ACO CIS security directive.

1-3. **DEFINITIONS. Security Infraction**. A Security Infraction is an act or omission, deliberate or accidental, which leads to a failure to conform to security regulations and/or the mandatory requirements of the AD 070-001. Such infractions can be considered either a procedural error or lapse, which has little impact on security and is not considered to have resulted in the compromise of NATO Classified Information (NCI). It should be locally recorded and investigated.

1-4. **Breach of Security.** A Breach of Security is an act or omission, deliberate or accidental, contrary to the AD 070-001, which has resulted in a threat to security or compromise of NCI. It should be recorded, investigated and reported. If in doubt then an incident shall be regarded as a Breach of Security.

1-5. **Compromise.** NCI is compromised when knowledge of it has, in whole or in part, passed to unauthorised persons and its confidentiality, integrity or availability has been impaired, i.e. individuals without appropriate NATO security clearance or authority to have access to said information. NCI, which is lost, outside a Security Area, even temporarily, is to be presumed compromised. Similarly, such unaccounted for information, even temporarily, inside a Security Area, including in recorded documents which cannot be located at periodic musters, shall be presumed compromised until a resultant investigation proves otherwise.

1-6. **Action on Security Incident.** All security incidents shall be reported immediately to the appropriate investigative authority Headquarters Security Officer (HQSO), to include, Allied Command Counter Intelligence (ACCI). In any cases where there are Counter Intelligence (CI) indicators, the Security officer must immediately notify supporting ACCI agents. Each reported incident is to be investigated by persons who have security, investigative and Counter Intelligence experience; whom are independent of those persons immediately involved in the incident.

1-7. **INVESTIGATIVE PROCEDURES.** The Security Officer of the relevant HQ or organisation is the person who is ultimately responsible for any investigation undertaken by the Security Office. Before conducting a security investigation (including conducting interviews) or taking any corrective action, the Security Officer must coordinate with supporting ACCI Special Agents. The security investigation should be divided into at least three phases.

1-8. **Phase I – Identification of the Type of Security Incident.** The aim of this phase is to ascertain what type of security incident took place (security infraction or breach of security) in order to allow investigative authority to choose the relevant procedure at the next phase of investigation. The diagram included in Annex X reflects procedures which should be followed on the first phase of any security investigation. If there is any doubt about the severity of a security incident then the investigating office shall contact SHAPE SEM J2X SPO.

1-9. **Phase II – Conduct of the Investigation.** HQSOs are to assess the scope of the investigation. If there are any CI indicators (espionage) then they shall contact ACCI and advise SHAPE SEM J2X SPO. ACCI is the only organisation specifically organised, staffed, equipped and authorised to conduct CI investigations within the NATO Command Structure (NCS). However, if ACCI do not wish to take on an investigation or the alleged offence does not meet the ACCI threshold for opening an investigation, then it is the responsibility of the HQSO to conduct that investigation to ensure that issues or security vulnerabilities that may surround the incident are captured and investigated. The diagram included in Annex Y stipulates relevant procedures that shall be implemented at this phase of security investigation. The aim of this phase is to determine if:

a. NCI has been threatened or compromised. If so, whether all the unauthorised individuals who have or could have access to the information have at least either a national or a NATO personnel security clearance and are known from existing records to be of such reliability and trustworthiness that no harm to NATO will result from the compromise.

b. Physical defences have been breached.

c. NATO assets have been removed, mishandled or damaged.

d. Impersonation has been attempted to gain access to NATO assets.

e. A suspected recce or other terrorist planning or action has taken place.

f. Other hostile action has been directed at NATO personnel and assets.

g. Any recommended remedial, corrective, legal or disciplinary action.

Furthermore, it is imperative that the conduct of any investigation follows the very highest of standards. Investigative procedures must be in line with the rule of law. Whenever an interview is conducted, any subject of the interview must be made aware of their rights BEFORE the commencement of the interview. Full investigative diaries shall be kept and any evidence handled in the correct manner. If HQSOs or investigators are unsure of how to proceed then they are to contact their Command LEGAD office and/or SHAPE SEM J2X SPO.

1-10. **Phase III – Reporting of Security Incident.** During this phase of investigation, respective procedures that shall be utilised dependent on the circumstances of the security incident. The diagram included in Annex Z describes the relevant procedures that shall be implemented at this stage of any security investigation.

1-11. **Role of the Principle/Command Security Advisor.** Regardless of the type of security incident, its seriousness and the classification of NATO information involved, at

each phase of security investigation ACCI and the Principle/Command's Security Advisor (PSyA/CSyA) shall be consulted. The PSyA/CSyA shall validate any assessments and conclusions of an investigation and provide advice on relevant courses of action. At each phase of a security investigation the PSyA/CSyA will coordinate all planning with supporting ACCI Special Agents. Furthermore, information concerning any adverse activity/records related to the individual(s) involved shall be requested from ACCI to provide Commanders with a true picture of said individual(s) attitude towards security. Particular caution should be taken with respect to security incidents where circumstances of the incident indicate suspected espionage or subversion (i.e. unauthorised gathering of NCI by individual(s) involved). Therefore, in all cases, PSyA/CSyAs shall coordinate with supporting ACCI Special Agents to ensure the proper inquiry of security incidents.

1-12. **REPORTING PROCEDURES. Reporting of Security Violations.** Where the investigation determines that no compromise of NCI has occurred, ACO commanders are the relevant Confirming Authority and, normally, can close such cases without recourse to higher authority. However, SACEUR retains the prerogative to review the result of any investigation and change the proposed actions and implement different or new ones when a violation has taken place systematically by the same individual(s) and with a significant number of documents. In these cases, SHAPE SEM J2, J2X SPO will inform the NOS and the national authorities of identified individuals. In any case, reports of investigation and remedial and corrective actions are to be kept for three years and are to be available during security inspections. Details of investigations should be included in the relevant organisation's Quarterly Security Return (QSR) (see Part IV, Chapter 2, Para 2-11 and Annex W).

1-13. **Reporting Breaches of Security.** Where the investigation shows that NCI may have been compromised, but that all unauthorised individuals who have or could have had access to the information have at least either a national or a NATO personnel security clearance and are known from existing records to be of such reliability and trustworthiness that no harm to NATO will result from the compromise, the local ACO Commander is the Confirming Authority and can close such cases without recourse to higher authority. However, SACEUR retains the prerogative to review the result of any investigation and change the proposed actions and implement different or new ones when a violation has taken place systematically by the same individual(s) and with a significant number of documents. In these cases, SHAPE SEM J2, J2X SPO will inform the NOS and the national authorities of identified individuals. Reports of investigation and remedial and corrective actions are to be kept for three years and are to be made available during security inspections. Details of all investigations undertaken should be included in the relevant organisation's QSR (see Part IV, Chapter 2, Para 2-11 and Annex W). This is to allow SHAPE SEM J2X SPO to undertake trend analysis into all security infractions, breaches etc. so that systemic security issues can be addressed.

1-14. **Reporting of Compromises.** Where the investigation reveals possible or confirmed compromise has occurred, an Immediate Report (within 48 hours) shall be forwarded through the chain of command to SHAPE SEM J2, J2X SPO to be forwarded to the NOS; ACCI are to be copied addressees to these reports. Where possible and appropriate, the reporting unit should inform ACCI and the originating unit at the same time as SHAPE SEM J2. The timing of the reports depends on the sensitivity of the information and the circumstances. Initial Reports shall be forwarded within 14 days to SHAPE SEM J2, J2X SPO through the chain of command in cases where it has been determined:

a. COSMIC TOP SECRET (CTS) or NATO SECRET information is involved, or

b. There are indications or suspicions of espionage (provided the report would not hamper the investigations in hand), or

c. Unauthorised disclosure to the press/media has occurred, or

d. Any loss or suspected compromise of NATO material by Non-NATO nations (NNN).

1-15. Immediate Reports shall contain the following details of compromise of NCI; however, there are no specific requirements regarding its format:

a. Date/time and location of incident.

b. Who reported the incident.

c. Description of the classified material involved including the security classification, originating formation, subject and scope.

d. A brief description of the known details of the incident.

e. The identification of the organisation investigating the breach of security.

1-16. Initial Reports should take the format at Annex AA and shall include:

a. Date/time and location of incident

b. Who reported the incident.

c. Full particulars of the individual responsible for the security breach, including service number, rank, nationality, full name and organisation.

d. Description of the classified material involved including the security classification, originating formation, subject and scope, file reference, copy number and date.

e. A brief description of the details of the incident: what happened, including who did what, where, when, why and how.

f. Description of the action taken to minimise the effects of any potential compromise, including the date that a damage assessment was requested from the originator and/or originating organisation

g. Identification of the organisation who is investigating the breach of security

1-17. **Final Report.** Reports on compromise of information classified NC and above shall be forwarded to SHAPE SEM J2 J2X SPO when the investigation has been completed. There is no requirement to report compromises involving information classified NATO RESTRICTED (NR) unless they meet the criteria set out paragraph VI-1-14 b. or c. above. In all cases of reportable compromise, the final report or a progress report of the investigation shall be sent to SHAPE SEM J2, J2X SPO within 60 days of report of the

breach. If the investigating authority cannot meet the 60 day deadline, then a request for extension should be sent to SHAPE SEM J2X SPO for endorsement.

1-18. Final reports should take the format at Annex BB and shall include:

a. A chronological summary of all relevant events.

b. The finalised assessment of the damage resulting from the breach. Any damage assessment shall include the methodology as well as the results.

c. Allocation of responsibility as a conclusion to the investigation assessing who or what directly contributed to the breach, e.g. human error or negligence and/or established procedure.

d. Description of corrective actions and recommendations made to prevent a recurrence.

e. Details of executive action, including the commander's opinion as to individual responsibility and the remedial action taken. If applicable, why remedial and corrective actions have not been taken and, if applicable, a request for relief from accountability for any missing material.

1-19. Breach of Security Initial and Final reports shall always be signed by the relevant Delegated Security Authority (Commander or Chief of Staff). The diagram in Annex Z stipulates the procedures and timelines for reporting of compromises of classified information.

1-20. **Remedial Action.** The primary purpose of remedial action is to engender, in a person whose act(s) or omission(s) are judged to have caused a security breach, a greater personal awareness of basic security practices. This can usually be achieved by a briefing from security staffs. However, in cases involving gross negligence or persistent offenders, ACO Commanders may have to carry out administrative or disciplinary action. In order that national authorities are kept aware of cases involving their personnel, the HQSO is to forward a copy of all reports to the formation national representative. In extreme cases, consideration is to be given to the denial of access to all NATO classified material, and to a request to the appropriate national authority for the individual's removal from the headquarters. The decision regarding this is at the discretion of each ACO commander as a Security Risk Owner.

1-21. **Confirming Authority.** The purposes of confirmation are to record formal sanction for the conduct of the investigation, agree the follow-up action and provide write-off powers for losses. The SHAPE Delegated Security Authority is the Confirming Authority for all security breaches (except ATOMAL), which are reportable in accordance with this directive. The NOS is the Confirming Authority for the closure of cases involving ATOMAL information.

1-22. **Records of Security Breaches,** including investigation reports and details of remedial and corrective actions taken, are to be kept for a minimum of three years, reported in the relevant QSR and are to be made available during security inspections.

1-23. **INVESTIGATIVE POLICY.** The purpose of a security investigation is to determine the extent of damage, actual or potential, to a NATO operation, activity, programme or

asset in order to assess any future action including mitigation of harm. The reporting outlined above will assist local and SHAPE SEM J2 staffs to take counter-compromise action, prepare institutional reparations, assess requirements for any disciplinary actions against those involved and compile security education material as appropriate.

1-24. Where an investigative agency has been called in to assist NATO with establishing the circumstances of a Breach of Security, that agency is to be invited to contribute to the reporting action detailed above. SHAPE SEM J2 and ACO Office of Legal Affairs (OLA) are to be notified when an external investigative agency is invited to participate in an investigation and should the agency concerned fail to contribute to the timely staff action on an incident, the matter should be reported to SHAPE SEM J2, who will coordinate engagement through the ACO OLA.

CHAPTER 2 – SECURITY INSPECTIONS

2-1. **ACO SECURITY INSPECTIONS.** All NATO Commanders are responsible for ensuring that the security measures are inspected periodically at each command level. The ACO Security Inspection Programme is a tool to assist Commanders to achieve and maintain a satisfactory standard of security. The main aim of a security inspection is to ascertain whether or not mandatory NATO security policy, procedures and standards have been implemented and to recommend corrective action where necessary. A secondary but equally important objective is to utilise the expertise of inspecting formations to advise on cost-effective and pragmatic solutions to meet the minimum NATO security standards.

2-2. Inspection priorities within ACO should be determined in the following order:

a. Category A - Headquarters in Deployed Operational Theatres.

b. Category B - Headquarters identified as having critical security deficiencies.

c. Category C - Headquarters holding CTS, ATOMAL and SIGINT NATO classified material.

d. Category D - Any other NATO organisation headquarters for which ACO has a security inspection responsibility.

2-3. **Inspection Responsibilities.** SHAPE ACOS SEM J2, on behalf of the ACO Security Authority is responsible for ensuring that NATO security standards are implemented throughout ACO. The ACO Security Inspection Programme is conducted under SHAPE ACOS SEM J2 oversight and direction.

2-4. SHAPE SEM J2X Security Policy Oversight (SPO) and Information Assurance (IA) inspecting team will inspect the security management functions of all subordinate headquarters, as well as each of their base support elements security functions. Similarly, each subordinate ACO Command J2X (or equivalent) SPO and IA inspecting teams are responsible for inspecting the security management and base support element security functions of their subordinate units. From time to time, SHAPE SEM J2X SPO and IA subject matter experts should join subordinate command inspection teams in order to validate inspection standards.

2-5. **Frequency of Inspections.** The frequency of ACO Security Inspections will be carried out as follows:

a. Category A Headquarters. Minimum twice per year.

b. Category B Headquarters. Within four months of the date of previous unsatisfactory report.

c. Category C Headquarters. Every 24 months.

d. Category D Headquarters. Every 36 months unless directed differently by SHAPE ACOS SEM J2.

2-6. Each ACO command J2X (or equivalent) shall develop their own Security Inspection Programme as agreed by their respective HQ COS. The Inspection Plan for the following year is to be submitted to SHAPE ACOS SEM J2 by 31 October.

2-7. **Security Advisory Visits (SAVs)** are conducted between security inspections and offer a less formal platform to augment the ACO security inspection programme. An SAV will focus on determining the progress of security inspection observations and recommendations, as well addressing new or emerging security issues. In addition, SAVs provide a support mechanism where ACO headquarters are formed, moved, disbanded or change role.

2-8. **METHODOLOGY.** Security inspections and intervening SAVs should be announced initially through the HQ Security Inspection Programme. Furthermore, a formal instruction should be sent from SHAPE SEM J2 J2X two months in advance of the inspection or SAV date in order to give the respective security personnel of the headquarter to be inspected an opportunity to make administrative arrangements to facilitate the visit. Ad hoc SAVs shall not require formal notification, nor be promulgated within the annual programme of work.

2-9. Inspection and SAV teams are to be formed at least 2 months in advance in order to ensure that the appropriate levels of experience in all the security disciplines under examination are covered. The inspection team shall consist of a nominated team leader and sufficient security staffs augmented by other specialists if necessary. The inspection team should not consist of personnel who have direct responsibility for the security of the headquarters to be inspected. An SAV shall normally consist of no more than 2-3 SME personnel.

2-10. The security inspection should be planned to meet specific objectives but should allow sufficient room for discretionary on site examination. Inspectors must observe the system in operation and assess whether the standard of security that has been achieved is consistent with the general aims of NATO Security Policy and the requirements of this directive. The requirements of headquarters' Internal Security Plans and supplements to this directive and other local security instructions are also to be taken into account.

2-11. In order that the security inspection team is able to obtain the facts as to whether the headquarters being inspected fulfils the requirements of NATO Security Policy and this directive, the inspecting team members shall:

a. Take into account the security classification and scope of the NCI held or used in any form in the inspected headquarter and review the sensitivity of this information and its vulnerability to compromise;

b. Identify the headquarters' security organisation directly responsible for establishing, implementing and enforcing the security regulations and procedures; and

c. After examination, determine whether the security protection satisfies NATO security requirements and is sufficient to provide adequate protection of NCI held within the inspected headquarters.

2-12. The security inspection team should conduct its examination and deliberations in frank and open manner and in full co-operation and consultation with the HQs security personnel and with responsible Command Group representatives. The security inspection team should not be confined to solely to checking all of the detailed points of the Internal Security Plans, local Supplements to this directive and other local security instructions but

should also satisfy itself that the implementation provides the necessary security protection to NCI to be protected as required by NATO Security Policy and this directive.

2-13. As far as possible, general information on the way security within inspected headquarter is organised shall be verified by spot checks, examination of files and records, visits to various areas, divisions and branches and interviews with individuals from various levels and activities, taking into account the particular security tasks for which they are responsible (i.e. Divisional Security Officers, Branch Security Officers, Divisional Control Officers, Terminal Area Security Officers, Cosmic and ATOMAL Control Officers). Where an HQ has difficulties in complying with a particular security requirement, the inspection team should be able to provide advice and suggest ways to attain the NATO security standards.

2-14. Inspections shall be graded in the following functional areas:

a. Security Organisation.

b. Physical Security.

c. Personnel Security.

d. Security of Information.

e. Information and Intelligence sharing with Non-NATO Entities (NNEs).

f. Security Procedures.

g. Security Awareness and Education.

2-15. For each of the above categories, a grading will be given as follows:

a. Unsatisfactory: The inspection team identified serious deficiencies in the security organisation of the headquarters; minimum standards of security are not being met and corrective actions are required.

b. Marginal: The inspection team identified deficiencies in security organisation of the headquarters; minimum standards are being met; however improvement is required.

c. Satisfactory: Minimum standards of security are being met, level of protection of NCI is acceptable in all respects.

d. Good: Denotes commendable standards.

2-16. The overall grading of each functional areas should be based on findings described in the checklist (Annex CC).

2-17. Should the inspected headquarter receive a grading of unsatisfactory in any of the functional security areas, a provisional overall grading of unsatisfactory shall be awarded. The inspected headquarter shall be given 30 days to rectify the deficiencies and report to the inspecting authority. Upon receipt of the Corrective Action Report, the inspecting authority will finalise the grading and release the Security Inspection Report. All finalised

Security Inspection Reports shall be forwarded to SHAPE ACOS SEM J2 for revision and acceptance by SHAPE Chief of Staff or his Delegated Authority.

2-18. **REPORTING PROCEDURES.** Verbal Report. At the conclusion of the security inspection, the team leader shall make a verbal report of the inspection results to Delegated Authority, or to his nominated representative from the inspected headquarters. This verbal report shall include details of any major security deficiencies noted and major problems discussed, as well as any recommendations concerning corrective actions. Where the inspection team leader believes that there is a need to make clear corrective actions to redress an unsatisfactory situation, he should annotate a copy of the inspection checklist for retention by the headquarters. In the event that the deficiencies revealed by the inspection are exceptionally serious, the inspecting authority shall inform SACEUR as soon as possible through the ACO chain of command.

2-19. Security Inspection Report. The inspection team leader is required to prepare a written report of the inspection. Where corrective actions or recommendations are included, sufficient details should be included in the report to support the rationale behind a corrective action, recommendation or observation. Corrective actions in the report shall be founded on relevant provisions of the NATO Security Policy. When the COS of the inspecting headquarter approves the Security Inspection Report shall be forwarded to the COS of the inspected ACO headquarters within 45 days of the inspection. When a security inspection is conducted at the level of operational or sub-units, the copy of the Security Inspection Report shall also be submitted to SHAPE ACOS SEM J2.

2-20. Upon receipt of the Corrective Action Report, the inspecting team leader shall finalise the Security Inspection Report in accordance with the format at Annex DD. If the inspected headquarters fails to meet the 30-day deadline, the inspecting authority shall release the report with an unsatisfactory grading overall.

2-21. Where ATOMAL information is involved, the Security Inspection Report shall be forwarded to the NOS, through SHAPE ACOS SEM J2.

2-22. SAV Report. An abridged SAV report providing a summary of findings shall be provided for each SAV conducted in between a security inspection. No grading will be appended to the SAV report, which shall be forwarded to the COS of the inspected ACO headquarters within 45 days of the advisory visit.

PART VII

CLASSIFIED PROJECT AND INDUSTRIAL SECURITY

CHAPTER 1: Introduction

CHAPTER 2: Tendering, Negotiation and Letting of Contracts/Sub-Contracts Involving NATO Classified Information

CHAPTER 3: Industrial Security Clearances

CHAPTER 4: Facility Security Officer

CHAPTER 5: Personnel Security Clearances

CHAPTER 6: Programme/Project Security

CHAPTER 7: Release of NATO Classified Information by Programme/Project Participants and Contractors/Sub-Contractors

CHAPTER 8: Handling of NATO Classified Information in Communication and Information Systems

CHAPTER 9: International Visit Control Procedures

CHAPTER 10: International Transfer and Transportation of NATO Classified Information and Material

CHAPTER 11: Glossary and Acronyms

This page is intentionally left blank.

CHAPTER 1 – INTRODUCTION

1-1. **General.** Industrial security is the application of protective measures and procedures to prevent, detect and recover from loss or compromise of NCI handled by industry in contracts. NCI disseminated to industry contractors and generated as a result of a contract shall be protected to a standard no less stringent than those set by NATO Security Policy (C-M(2002)49) and supporting Directives.

1-2. This part of the ACO Security Directive contains mandatory minimum security standards, common procedures and processes in connection with the implementation of industrial security within ACO.

1-3. **Scope.** This part of the ACO Security Directive applies to the protection of NCI released or created during all phases of the contracting processes, including licensing, bidding, negotiation, award, performance (e.g. construction[16]), and termination. The protection of NATO UNCLASSIFIED (NU) information is governed by C-M(2002)60, The Management of Non-Classified Information, and is addressed in this part only for completeness.

1-4. **Definitions.** The provisions outlined in this part are based on AC/35-D2003-REV5 Directive on Classified Project and Industrial Security, which are applicable to NATO, NATO Programme/Project Agency/Offices (NPA/NPOs), ACO Programme/Project Offices (APOs), National Security Authorities (NSA), Designated Security Authorities (DSA), Security Accreditation Authorities (SAAs) and any other competent NATO and national authorities that let contracts involving NCI to Contractors. The following definitions apply:

a. ACO Contracting Authority. An ACO component commander or his Delegated Authority authorised to tender for, or place a contract with a Contractor, Consultant or Sub-Contractor.

b. ACO Programme/Project Office (APO). An office designated within an ACO component that is responsible for the overall management of the programme/project for its ACO Contracting Authority.

c. APO Security Manager (APOSM). An APOSM is responsible for planning and execution - in cooperation with relevant HQSOs, NSA/DSA/SAA, contractor's FSOs and all other programme/project/construction stakeholders - of all aspects of security, CIS security and Force Protection during all stages of the programme/project/construction, in accordance with security principles described in this Directive.

d. Contractor. An industrial, commercial or other entity that seeks or agrees to provide goods or services.

e. Consultant. An individual who serves either independently or through a Contractor in an advisory capacity. A Consultant expresses views, gives opinions on problems, answers questions as requested, or provides advice. The work

[16] 'Construction' includes building and installation renovation alteration, refurbishment, replacement, modification and major repair works.

performed under contract is the provision of advice. Therefore, for the purpose of this Directive, a Consultant is considered the same as a Contractor.

1-5. **Authority.** The ACO Security Authority and his Delegated Security Authorities within ACO components, NSAs/DSAs and the relevant Security Accreditation Authorities (SAAs) are responsible for the security of NCI entrusted to the Contractors under their jurisdiction. They exercise the security supervision over the Contracting Authorities and the respective Contractors established under their jurisdiction.

1-6. Similar to procedures on Information and Intelligence Sharing with Non-NATO Entities, each ACO component headquarters' Security Authority is responsible for the management of risk related to sharing NCI with non-NATO participants of classified programmes/projects. Physical access to security areas within ACO component headquarters, access to NATO or NATO/X classified CIS, access to NCI and release of NCI to Non-NATO participant of classified programme/project shall be based on a written decision of the relevant ACO component Security Authority.

1-7. An ACO component Security Authority may delegate responsibility on risk management related to information-sharing in the framework of classified programmes/projects to the head of APO. Subsequently, the APOSM will be nominated Programme/Project Security Advisor (ProSyA).

1-8. Detailed responsibilities of the APO, NSAs/DSAs, and the NOS are laid down in Annex EE. Principle organisations with responsibility for CIS security (e.g. SAAs) are addressed in Enclosure F to C-M(2002)49-REV1.

CHAPTER 2 – TENDERING, NEGOTIATION AND LETTING OF CONTRACTS/SUB-CONTRACTS INVOLVING NATO CLASSIFIED INFORMATION

2-1. **CONTRACTS/SUB-CONTRACTS IN NATO NATIONS – GENERAL.** All Contractors/Sub-contractors undertaking an ACO contract involving NCI who require access to or generate information classified NC and above, shall hold or, in respect of paragraph 11 (b) and (c) below, be able to obtain an FSC at the appropriate level issued by the responsible NSA/DSA of the country that has jurisdiction[17] over the Contractor/Sub-contractor's facility. It is the responsibility of the APO to verify with the relevant NSA/DSA of a Contractor/Sub-contractor whether it has been granted an appropriate FSC before any NC or above information is released to it. Where no FSC at the required level exists, it is the responsibility of the relevant APO to initiate an FSC or upgrade action.

2-2. A FSC is not required by Enclosure G to C-M(2002)49-REV1 for access to, or generation of information classified NR. However some NATO nations, as mandated by their national laws and regulations, do require a FSC for Contractor/Sub-contractor under their jurisdiction, for access to information classified NR.

2-3. **TENDERING PROCESS.** Access to Information Classified NATO CONFIDENTIAL and above during the Tendering Process. A bidder, not holding an appropriate FSC as required by the potential contract/sub-contract shall not be automatically excluded from the competition during the tendering process, as detailed in the scenarios below.

a. The following identifies the three scenarios that may arise during the tendering process for a contract/sub-contract involving information classified NC and above and details the security requirements:

(1) Access to information classified NC and above at the bidder's facility during the tendering process:

(a) When the contract notice, invitation to tender or request for proposals require bidders to hold or generate at their facility information classified NC and above, the bidder's facility shall hold an FSC at the appropriate level. In such circumstances the APO shall obtain a confirmation from the relevant NSA/DSA that the bidder has been granted an appropriate FSC.

(b) The APO shall obtain the respective confirmation from the responsible NSA/DSA by using the FSC Information Sheet (FSCIS).

(2) No access to information classified NC and above during the tendering process:

(a) When the contract/sub-contract notice, invitation to tender or request for proposal concerns a contract/sub-contract that will involve classified information NC or above but does not require the bidder to hold or originate such information at the tender stage, a bidder not holding an appropriate FSC shall not be excluded from the bidding process, but should be advised in the tender document that an FSC

[17] Power to exercise authority over a subject matter or a territory/geographic area.

shall be required at the moment of being awarded the contract/sub-contract.

(b) Should a bidder without an appropriate FSC be selected to undertake the contract/sub-contract, the APO shall initiate action to grant the bidder an FSC at the required level before the contract/subcontract is awarded.

(c) The contract/sub-contract shall not be awarded until the NSA/DSA has provided a confirmation that the selected bidder's facility has been granted an FSC at the required level. The APO shall initiate the FSC action by using the FSCIS at Annex FF. Exceptionally, and after consulting with the relevant NSA/DSA, the APO may allow the Contractor to commence work on the NR parts of the contract, provided the contractual arrangement includes a clause stating that the contract shall be terminated in case the Contractor cannot be granted the required FSC.

(3) Access to information classified NC and above at the premises of the ACO component during the tendering process:

(a) Shall only be granted to individuals who are in possession of an appropriate Personnel Security Clearance (PSC). An assurance of the PSC of individuals requiring physical access to Security Areas within the premises of ACO components shall be provided only in the form of a PSC Confirmation or a Request for Visit (e.g. for Contractor personnel) by the appropriate NSA/DSA. All other forms of assurance such as a copy of a PSC shall not be accepted;

(b) Shall not be granted in case a bidder without an appropriate FSC is selected to undertake the contract/sub-contract before the assurance from the relevant NSA/DSA, that the bidder has been granted an appropriate FSC at the required level has been obtained by the APO; and

(c) The contract/sub-contract shall not be awarded until the NSA/DSA has provided an assurance that the selected bidder's facility has been granted an FSC at the required level. The APO shall request the responsible NSA/DSA initiate the FSC action by using the FSCIS at Annex FF.

b. Should the NSA/DSA determine that a bidder is ineligible for the required level of FSC, the relevant ACO Contracting Authority shall not award the contract.

2-4. Access to Information classified NATO RESTRICTED during the Tender Process. When the contract notice, invitation to tender or request for proposals require bidders to hold or generate NR information, the contract notice, the invitation to tender or request for proposal shall include a copy of the "Contract Security Clause for Inclusion in Tenders and Contracts Involving NR Information" at Annex GG. This will inform the bidder on the minimum measures required for the protection of NR classified information.

2-5. **Unsuccessful Bidders.** Unsuccessful bidders having been provided NCI in connection with a tender shall be required to return the NCI to the APO within 15 working days of receipt of notification of their unsuccessful tender. All individuals having accessed NCI shall be reminded of their responsibility for its protection and of not disclosing such information further.

2-6. **NEGOTIATIONS.** Following the bidding process and at the start of negotiations for contracts involving information classified NC or above with preferred bidders, if not already confirmed, a confirmation shall be obtained that the potential Contractor holds an FSC at the required level. The APO shall forward request for such a confirmation to the NSA/DSA with jurisdiction over the potential Contractor.

2-7. The APO shall ensure that all Contractors are required to follow the same approval process when negotiating a sub-contract.

2-8. The APO shall also provide information regarding the security classification level of the information processed, generated or held by the contractor, the contract period and the nature of services or supplies requiring access or potential access to NCI to the responsible NSA/DSA. The responsible NSA/DSA shall be provided with all the information required to ensure that the necessary security arrangements have been implemented and will be maintained throughout the lifecycle of the respective classified programme/project/construction contract.

2-9. **CONTRACTS.** Contracts involving Information classified NATO RESTRICTED. Contracts involving information classified NR shall include a “Contract Security Clause for Tenders and Contracts Involving NR Information” detailing, as a minimum, the provisions specified in Annex GG. Such contracts shall also include a Security Aspects Letter (SAL) (see Annex HH) identifying the specific NR aspects of the contract requiring protection.

2-10. The requirements in contracts for the protection of NR information may be more stringent than that detailed in Annex GG and, if required by national laws and regulations per Annex II, NSAs/DSAs will be responsible for ensuring compliance of Contractors/Sub-contractors being under their jurisdiction with applicable security provisions for the protection of NR information and should conduct verification visits on Contractor’s facilities located in their nation. In all other cases it is the responsibility of the APO to ensure that the required security provisions of Annex GG and the SAL, as applicable, are implemented. Any incident, which has or may lead to NR information being lost or compromised, shall immediately be reported to the APO and the Contractor’s NSA/DSA, as applicable.

2-11. Contracts involving Information classified NATO CONFIDENTIAL and above. Contracts involving access to information classified NC and above shall include an article, which requires the Contractor to protect any such NCI no less stringently than applicable NATO security regulations as implemented by its competent NSA/DSA, and comply with any relevant national security laws and regulations and any additional instructions given by the responsible NSA/DSA. Contract specific NATO security requirements shall be given either in a Programme (Project) Security Instruction (PSI) (see Annex JJ) or in a SAL, as appropriate.

2-12. **Performance of Contracts within ACO Component Class II Security Areas.** Unescorted access to Class II Security Areas within ACO component headquarters shall only be granted to Contractor’s employee who are security cleared up to NS. For

Contractor's employees without appropriate PSC, provisions shall be made for escorts or equivalent controls to prevent unauthorised access to NCI. If escort arrangements or equivalent controls are not feasible, the requirement for individuals to hold an appropriate PSC when the execution of the contract starts shall be clearly stated in the invitation to bid. Physical access to Class II Security Areas within ACO component headquarters by Contractor's employee shall be based on a decision made by the headquarter Security Authority or, when such authority is delegated, by the head of APO. Such a decision shall be based on justification provided by the Contractor's Facility Security Officer and reviewed by the APOSM. Justification of the request should take into account such factors as nationality, level of PSC, nature of the contract and requirement for escorted or unescorted access. Such an access may be granted for the duration of the contract if required. Requirement for physical access to an ACO component headquarters Class II Security Area by Contractor personnel shall be constantly monitored by the HQSO, in connection with the APOSM, and shall be withdrawn immediately when it is no longer required.

2-13. **Programme/Project Security Instruction (PSI) and Security Aspects Letter (SAL).** For all programmes involving information classified NC and above, managed by an APO the APOSM shall produce a PSI (see Annex JJ) in collaboration with NSA/DSA of the NATO nation(s) participating in the programme and subject to approval by the relevant ACO component Security Authority. Security classifications of the programme or project shall be addressed in the Security Classification Guide (SCG). If considered appropriate by the programme/project participants (i.e. when aggregation of NR information occur) a PSI may also be required for programmes/projects involving only NR information.

2-14. Contracts which do not require a PSI shall include as a minimum an SAL. In that case security classifications shall be addressed in attached Security Classification Checklist.

2-15. The PSI and/or SAL shall be made binding for all programme/project participants.

2-16. **Notification of Contracts.** APOSM shall notify the NSA/DSA with jurisdiction over the Contractor about any contracts involving NCI at the level of NC and above, to include details on the nature of services or supplies or work to be performed by the Contractor, the security classification, the nature and volume of classified information to be provided to or to be generated by the Contractor, as well as any other relevant security aspects.

2-17. Each APO shall develop and maintain an up-to-date list of facilities and involved organisations. The list shall be in the format at Annex KK and shall consist of:

a. The prime Contractors that hold contracts involving classified information NC and above connected with the ACO programme/project;

b. All government departments or agencies known to be involved in the programme/project/construction; and

c. Any civil or military body involved, when applicable.

2-18. Each APO shall also be responsible for requiring that each prime Contractor maintains a similar list for any Sub-contractors, by programme/project, with access to information classified NC and above.

2-19. Other Contracting Authorities awarding a NATO classified prime contract involving NCI at the level of NC and above, will provide their respective NSA/DSA with a copy of the security provisions of the contract and the PSI/SAL. That NSA/DSA will provide copies of the security provisions and PSI/SAL to the NSA/DSA of the country with jurisdiction over the Contractor so that security oversight of the NCI can be maintained.

2-20. **Contracts/Sub-Contracts with Contractors in Non-NATO Nations.** The letting of the contract involving NCI to Contractors in Non-NATO Nations (NNN) constitutes a release of information and shall be in accordance with the established procedures as referenced in paragraph 6-1. Release of NCI originated within ACO to contractors in NNNs shall always be based on a risk assessment and decision made by the relevant Security Authority or, when this authority is delegated, by the head of APO. Each release shall be reviewed and advised by APOSM.

2-21. Contracts/sub-contracts with Contractors/Sub-contractors in NNN which involve NCI require the existence of a bilateral Security Agreement between NATO and the NNN, whose NSA/DSA has jurisdiction over the Contractors/Sub-contractors. It is the responsibility of that NSA/DSA to ensure their Contractors/Sub-contractors provide the required level of protection for the contract involving NCI.

2-22. If there is no Security Agreement between NATO and the NNN, a bilateral Security Agreement between a contracting/sponsoring NATO Nation and the subject NNN is required. The contracting/sponsoring NATO Nation shall provide the ACO component Contracting Authority a written Security Assurance signed by a representative duly mandated by the non-NATO recipient. The Security Assurance shall oblige the NNN recipient to protect NCI to a degree no less stringent than the provisions contained in the bilateral Security Agreement for the protection of the NATO Nation's classified information of an equivalent classification.

2-23. If the NATO Nation which has concluded the Security Agreement with the NNN does not have the jurisdiction over the Contractor, the NSA/DSA of the NATO Nation with jurisdiction over the contractor will provide the Security Assurance as detailed in paragraph 2-20 above, together with a copy of the Security Agreement. The written consent of the NATO Nation with jurisdiction over the contractor is required otherwise the contract shall not be placed.

2-24. Placing contracts/sub-contracts involving NCI shall follow the procedures as established in paragraphs 2-1 to 2-17 above.

2-25. **Termination of Contracts involving Classified Information.** Upon termination of a contract/sub-contract involving classified information, and where NCI has been provided to or generated by the Contractor/Sub-contractor during the performance of the contract, the information/material shall be returned to the APO unless the head of APO has agreed in writing that the NCI released can be destroyed in accordance with the national laws and regulations or retained by the Contractor/Sub-contractor, e.g. for purposes of follow-on services or supplies. Disposition instructions shall be included in PSI to any contracts involving release of information classified NC and above. The relevant APO shall be provided copies of Destruction Certificates of all accountable NATO classified documents and items originated within ACO and released to Contractor/Sub-contractor.

CHAPTER 3 – INDUSTRIAL SECURITY CLEARANCES

3-1. **Facility Security Clearances.** The NSA/DSA of each NATO nation is responsible for granting an appropriate FSC for Contractor's facilities under their jurisdiction and which are involved in NATO contracts involving information classified NC and above, in accordance with national laws and regulations. Prior to granting an FSC, an assessment is made on the following mandatory minimum requirements:

a. Of the integrity and probity of the company which is to be entrusted with NCI at the level of NC and above;

b. Of the personnel security status of owners, directors, principal officials, executive personnel, and employees of the facility, and of such other individuals as per national laws and regulations who may, by virtue of their association, position or employment, be required to have access to NCI or supervise a NATO contract involving NCI, to ensure that they have the requisite level of PSC;

c. Of the foreign ownership, control and influence aspects (such as corporate structure) to ensure that these aspects are adequately addressed and where necessary mitigated; and

d. Of the security arrangements provided for the protection of NCI to ensure that they comply with the requirements of NATO Security Policy.

3-2. An FSC is an administrative determination by which an NSA/DSA formally recognises the capacity or reliability of Contractor's facilities to manage, generate or have access to NCI up to a certain level. Depending on the contract requirements and, subject to national laws and regulations, there may be different types of FSCs, as determined by the NSA/DSA and are conveyed in the NATO FSCIS.

3-3. The following minimum criteria are applied by the NSA/DSA in issuing all categories of FSCs:

a. That the company must establish security processes which cover all appropriate security requirements for the protection of information classified at NC and above in accordance with NATO security regulations;

b. That the personnel security status of personnel (both management and employees) who are required to have access to information classified NC and above is confirmed in accordance with NATO PSC requirements;

c. That the NSA/DSA has the means to ensure that the industrial security requirements are binding upon the contractor company and that it has the right to inspect and approve the measures taken within the contractor company for the protection of information classified at NC and above; and

d. That the contractor company shall appoint a Facility Security Officer (FSO) responsible for all aspects of security, CIS security and Force Protection, who is in a position to report to the NSA/DSA.

3-4. Typical categories of personnel being subject to the security clearance procedure, in relation to the issuing an FSC, are:

a. Owners of companies, members of supervisory boards and members of management boards who may be subject to the PSC process in accordance with requirements in national laws and regulations, or who may be the members of the management the FSO is reporting to;

b. FSOs, CIS Security staff, registry staff, couriers and SMEs of the contractor company may be subject to the PSC process as required for the fulfilment of the contract involving NCI.

3-5. In granting an FSC, NSAs/DSAs ensure that they have the means to be advised of any circumstances that could have a bearing upon the viability of the clearance granted (e.g. a transfer of the controlling interests in the company or facility, a realignment of the business associations, the replacement of any of its principal officers or directors, a change in the facility's physical location, an alteration to the premises it occupies, or a variation in its security procedures).

3-6. The NSAs/DSAs evaluate the extent to which the circumstances described above represent a threat to the security of NCI that may be entrusted to that contractor, company or facility. If it is determined that there is a threat, the NSAs/ DSAs will take appropriate steps to negate or mitigate the threat prior to issuing the FSC.

3-7. The responsible NSA/DSA shall confirm the level of the FSC granted, or initiate facility clearance action for a company, when requested, in the FSCIS format (connect Annex FF).

3-8. The NSA/DSA may specify additional security measures to be taken for the protection of NCI in each contractor company facility in its nation in order to qualify for an FSC.

3-9. **Contractor Personnel Performing Work on ACO Component Premises or on Other Contractor Facilities.** Contractor/Sub-contractor personnel, including freelance consultants and interpreters, or any other type of freelance personnel or self-employed service providers who carry out works on ACO component premises, or Contractor facilities in connection with a classified NATO programme/project, or any other type of NATO contract requiring access to information classified NC and above, shall hold a PSC at the requisite level. An appropriate FSC for the Contractor/Sub-contractor might be required by national laws and regulations.

3-10. **Changes to or Revocation of FSC.** Should an NSA/DSA change or withdraw an FSC that it has issued, the NSA/DSA will at once notify the APO and any other relevant entity to which it has provided an FSC confirmation. The contractual arrangement shall include a clause stipulating that the revocation of the required FSC shall constitute a reason for termination of the respective contract without reimbursement to the Contractor or claim against APO.

3-11. Similarly, APO shall immediately notify the requisite NSA/DSA if any reasons are observed to revoke a Contractor/Sub-contractor's PSC or FSC.

CHAPTER 4 – FACILITY SECURITY OFFICER

4-1. **General.** A Contractor/Sub-contractor's Facility Security Officer (FSO) should be in place, responsible for overall protection of received NCI related to the programme/project. This appointee is obliged to ensure the effective implementation of security procedures within the facility granted FSC.

4-2. The FSO will serve as the main point of contact between the Contractor/Sub-contractor, the APO and relevant NSA/DSA for all security related aspects of the contract. When appointing the FSO, the following requirements apply:

a. The FSO shall be:

(1) A citizen of the nation where the contractor facility is located, or a citizen of a NATO nation (for contracts involving information classified NC and above);

(2) An employee of the Contractor/Sub-contractor;

(3) Granted a PSC at the appropriate level;

(4) A part of the facility management, or reporting directly to one of the members of the management in order to exercise security authority.

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

c. The responsible NSA/DSA shall maintain a close cooperation with the FSO.

4-3. **Responsibilities.** The FSO shall also be responsible for the following tasks:

a. Establishing and maintaining a system of procedures and measures for the protection of NCI. These measures will ensure that all security requirements specified for personnel security, physical security, security of information and CIS security are adhered to and are in place throughout the lifetime of the classified programme/project.

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 programme/project/construction, changes to physical security, security of information and CIS security, 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 and warning the APOSM on any suspected espionage, sabotage or subversive activities at the facility, including any indication of loss, compromise or suspected compromise of NCI and any other security risks concerning NCI.

d. Providing initial security briefings to new employees before they are given access to NCI. Providing annual security training and security awareness programs for all personnel with access to NCI, and conduct debriefings with individuals who

are terminating employment on their continuing responsibilities concerning the safeguarding of NCI they have accessed (a letters of acknowledgement shall be signed).

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 incidents, submit an initial investigation report of the security incident and final report including the corrective actions taken to the responsible NSA/DSA and informing the APO.

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

CHAPTER 5 – PERSONNEL SECURITY CLEARANCES

5-1. **General Provisions.** All individuals Contractors/Sub-contractor's personnel (e.g. freelance consultants, interpreters, or any other type of freelance personnel or self-employed service providers) whose functions may afford or require access to information classified NC and above or unescorted access to Class I or Class II Security Areas, shall be appropriately security cleared and briefed before such access is authorised. Individuals shall only have access to NCI to which they have a clearly established need-to-know, which shall be confirmed by the FSO.

5-2. A PSC is not required for access to NR information; individuals shall have a need-to-know, shall be briefed about their responsibilities for the protection of NR information and shall acknowledge in writing that they fully understand their responsibilities.

5-3. Personnel security is addressed further at Enclosure C to C-M(2002)49-REV1 and in the supporting Directive on Personnel Security AC/35-D/2000.

5-4. **Contractual Conditions.** Before letting a sub-contract involving information classified NC or above the Contractor will contact the responsible APO seeking the Contracting Authority's approval for the decision in relation to the chosen Sub-contractor. The APO shall contact the responsible NSA/DSA to ensure that the Sub-contractor's facility and personnel requiring access to NATO information classified NC or above fulfil the requirements of this Directive.

5-5. **Initiating Personnel Security Clearance Procedures.** The FSO will request each individual requiring access to information classified NC and above to complete the respective national PSC questionnaire and forward the completed form to the responsible NSA/DSA.

5-6. **Renewal of PSCs.** The FSO will be responsible with ensuring the timely processing of a request for renewal of the employee's PSC with the responsible NSA/DSA.

5-7. If a PSC is not renewed within the validity period of the clearance, and when the respective NSA/DSA confirmed that revalidation process is commenced and that there are no adverse information on individual's reliability and trustworthiness, the head of responsible APO may allow an individual's access to NCI to be extended for a period of 6 months. Such a decision shall be taken by the head of APO every 6 months until the PSC is renewed.

5-8. **PSC of an Employee Holding the Nationality/Citizenship of Another Nation.** If a PSC is required for a Contractor/Sub-contractor employee whose nationality/citizenship is that of another NATO nation, the NSA/DSA of the nation which has jurisdiction over the Contractor will obtain a PSC or assurance from the employee's country of nationality/citizenship.

5-9. As an alternative, having the character of subsidiarity, the NSA/DSA which has jurisdiction over the Contractor may, where permitted by national laws and regulations, grant a PSC to an employee holding the nationality/citizenship of another NATO nation provided that:

a. The employee has resided in the Contractor's country for at least 5 consecutive years;

b. The NSA/DSA of the nation which has jurisdiction over the Contractor have checked their appropriate records to ensure that there is no adverse information;

c. The material and information concerned with the contract is not at the CTS level; and

d. An assurance is requested from the NSA/DSA of the employee's country of citizenship that there is no adverse information in respect to the individual that would prevent the granting of a PSC by the parent nation.

5-10. If a Contractor/Sub-contractor facility wishes to employ a citizen of a non-NATO nation in a position that requires access to NCI, it is the responsibility of the NSA/DSA which has jurisdiction over the hiring facility to determine the suitability of the individual for accessing NCI in accordance with NATO standards.

5-11. **Multiple Nationalities.** For individuals holding multiple nationalities, where appropriate, the NSA/DSA of the nation granting the PSC will obtain an assurance on the individual's suitability to be granted a PSC from the other nations, subject to the applicable national laws and regulations.

5-12. **Provisional PSCs.** The NSA/DSA may issue a provisional PSC in accordance with its national laws and regulations. The period of validity of such a PSC and its level will be determined and confirmed by the issuing NSA/DSA.

5-13. In exceptional cases, where the fulfilment of major operational objectives would otherwise be seriously impaired, and it is not possible to obtain the PSC in time by prioritising a particular request, access may be permitted by head of APO. However, such access may be permitted only with the prior approval of the originator, be limited only for citizens of NATO nations, and in connection with contracts requiring access to NCI not higher than NS.

5-14. **Confirmation of PSCs.** The verification that the individual has a valid PSC may either be in the form of Request for Visit (RFV) (Tab 2 to Appendix 1 of Annex S), or in the form of the PSC Confirmation (PSCC) (connect Annex R).

5-15. **Security Awareness and Briefings of Individuals.** All Contractor/Sub-contractor individuals conducting their work within the ACO component headquarters where they have access to NCI, shall be briefed on security procedures and their security obligations. All individuals having access to NCI shall acknowledge that they fully understand their responsibilities and the consequences which the law or administrative or executive order of their nation provides when classified information passes into unauthorised hands, either by intent or through negligence. A record of the acknowledgement (ACO Form 107 or acknowledgement letter) shall be maintained by the relevant APOSM.

5-16. Within ACO component headquarters, similarly to the ACO personnel, all Contractor/Sub-contractor individuals who are authorised access to, or required to handle NCI, shall initially be made aware, and periodically reminded, of the dangers to security arising from indiscreet conversation with persons having no need-to-know, their relationship with media, and the threat presented by the activities of intelligence services which target NATO and its member nations. Individuals shall be thoroughly briefed on these dangers and must report immediately to the appropriate APOSM, HQ SO or ACCI any approach or manoeuvre which they consider suspicious or unusual.

5-17. Within ACO component headquarters, all Contractor/Sub-contractor individuals who cease to be employed in duties requiring access to NCI shall be made aware of, and acknowledge, their responsibilities for the continued safeguarding of NCI (ACO Form 107 or acknowledgement letter).

5-18. **Procedures to be Followed When a PSC is Altered, Suspended or Revoked.** If the NSA/DSA with jurisdiction over the Contractor/Sub-contractor becomes aware of adverse information about an individual who is a national of another NATO Nation, it will inform the NSA/DSA of the individual's country of citizenship in order to determine whether the individual shall continue to hold a PSC.

5-19. In the case where an NSA/DSA that issued a PSC for an individual decides to alter, suspend or revoke the individuals PSC, it will immediately inform the relevant APO, NSA/DSA and any other body to whom the individuals PSC Confirmation has been provided, as well as the NSA/DSA of the nation of origin of any facility that requested a PSC for the concerned individual.

5-20. On receiving the information that a PSC has been altered, suspended or revoked, the APOSM of the ACO component headquarter, which employs the individual, shall ensure that the individual is denied access to headquarters Security Areas, access to NCI and has also been security debriefed.

5-21. The contractual arrangement shall include a clause stipulating that the alteration, suspension and/or revocation of the PSC shall constitute a reason to terminate the respective contract without reimbursement to the Contractor, or claim against APO, or the said nation if the timely access to NCI classified NC or above is required to fulfil the contractual obligation.

5-22. **Procedures to be Followed When a PSC is Denied.** The NSA/DSA with jurisdiction over the Contractor/Sub-contractor will inform the APO of the ACO component headquarter where the individual is employed of the denial of a PSC. If other NSAs/DSAs have been involved in the PSC process they will also be notified of the denial of the issuing of the PSC.

5-23. Should the NSA/DSA of a parent nation of an individual decide not to grant a PSC, it will immediately inform the NSA/DSA of the nation which has jurisdiction over the facility that requested the PSC.

5-24. Equally, should the NSA/DSA of the nation with jurisdiction over the Contractor/Sub-contractor that requested the PSC decide not to grant it for employed individual, it will immediately inform the NSA/DSA of the individual's country of citizenship.

5-25. On receiving the information that a PSC has been denied, the APOSM of ACO component headquarter which employs the individual shall ensure that he is not involved in any classified work at the level of NC and above, and his unescorted access to Security Areas within the HQ is revoked.

This page is intentionally left blank.

CHAPTER 6 – PROGRAMME/PROJECT SECURITY

6-1. **Introduction.** Where established, the ACO component Programme/Project/ Construction Office (APO) is responsible for managing project security for major NATO programmes/projects/constructions or procurement activities. The security risks related to the operational, technological, political and commercial sensitivities of the project must be considered, and although these risks are managed by the APO, individual programme participants (the security stakeholders) shall be made aware of identified security risks.

6-2. **Security-by-Design.** Within ACO components, the relevant APOs managing construction work within their establishments shall consider two critical construction security concerns related to the Security-by-Design[18] principle. Whereas the first identifies security aspects related to design process, as well as to contracting, execution, and reception of construction works, the second identifies security related topics that shall be implemented in the construction works to follow the NATO Security Policy standards in the completed construction works, during planned use, as well as during normal repair and maintenance activities. By ensuring implementation of NATO Security Policy standards at the start of construction works, the APO will optimise collaboration and compatibility between security, design, and construction requirements.

6-3. **Programme/Project/Construction Security Instructions.** At the start of a programme/project/construction it is important to define the process required to ensure effective management of security throughout the activity, primarily by identifying and recording the relevant security sensitivities and identifying the appropriate protection in a Programme/Project/Construction Security Instruction (PSI). All participants are responsible for the implementation of security requirements set by the PSI. It is also important to ensure that the security requirements for the programme/project are kept up-to-date during the entire life of the programme/project/construction.

6-4. For the programme/project/construction where an ACO component commander is a Contracting Authority the PSI shall be developed by the APOSM in coordination with local HQSO, relevant NSA/DSA and Contractor/Sub-contractors' FSO, and approved by the headquarters' Security Authority or, if this authority is delegated, by the head of APO.

6-5. The allocation of a NATO security classification indicates the required level of protective security to be provided to material or information associated with the NATO programme/project/ construction and the expected impact or damage to NATO as a consequence of loss or compromise associated with programme related NCI or classified material. Release of NCI related to classified programme/project/construction, originated within an ACO component shall always be based on a written decision of the relevant Delegated Security Authority or, if this authority is further delegated, the head of APO.

6-6. **Principles.** Security measures are established to deter, detect and prevent the compromise of NCI and protect its confidentiality, integrity and availability. Within programme/project/construction security, it is important to recognise that such security measures are not only required for the technological aspects of the material, but also

[18] Security-by-Design is a policy principle to ensure that security is embedded from the outset of any work related requirement (e.g. new build/construction programmes/projects) through the initial planning, implementation and subsequent lifecycle of the requirements. It aims to enable and positively influence security based on number of core elements, including customer focus, environmental understanding, security application 'up front', risk assessment and management, natural security, creativity and compliance.

aspects such as how the material is to be used, where it will be used, details of the acquisition programme (e.g. prices, dates, quantities, etc.), and consideration of the need for associated specific information/data (e.g. mission plans, intelligence data libraries) or material (e.g. specific radios for interoperability). When considering the security risks to the programme/project/construction, attention needs to be given to any operational, technological, commercial and political risks. Depending on the nature of the classified programme/project/construction the related threat assessment should be based on analysis provided by SMEs in various disciplines, such as technical, intelligence, security, or foreign disclosure.

6-7. Following determination of the threats and vulnerabilities associated with the programme/project/construction, security is achieved by:

a. Security classification of information. The security classification applied is appropriate to the state of development of the programme/project/construction. The preparation of a Security Classification Guide (SCG) requires collaboration amongst the programme/project/construction technical staff and security professionals. The SCG shall be in form of Annex to PSI and is one of the most important tools in preparing of the programme/project/construction related documents.

b. Once the correct security classification of the programme/project/construction is defined, the corresponding security marking shall be explicit and without deviations, determining and applying the correct security marking of NCI in the context of the specific programme/project/construction and applying the PSI and the SCG in the form of mandatory Programme (Project/Construction) Marking Instructions (PMI).

c. Need-to-Know. This principle is to be adhered to by all personnel involved in handling or generation of NCI in the context of a programme/project/construction.

d. The applicable security protection of a programme/project/construction should be reviewed regularly by APO at each programme/project/construction approvals milestone, to ensure its consistency and effectiveness.

6-8. For all programmes/projects/construction managed by APO component involving information classified NC and above, a PSI shall be developed utilising the template at Annex JJ. The purpose of the PSI is to supplement the security policies and requirements detailed in this ACO Directive. It shall establish specific security procedures associated with the NATO programme/project/construction concerned and assign responsibilities for the implementation of security measures concerning NCI generated and exchanged under the development, production and follow-on support of the NATO programme/project/construction. If considered appropriate by the APO and programme participants a PSI may also be produced for programmes involving only information below NC. The PSI should also include security marking and handling instructions for unclassified information.

6-9. For the ACO component led programme/project/construction the PSI shall be developed by the APO in conjunction with the relevant NSAs/DSAs FSOs and technical staff if required. It shall include an SCG which must identify the security sensitivities and security classification of the aspects related to the programme/project/construction, as well as a binding PMI.

6-10. The PSI shall apply to all military and civilian establishments and as described below to Contractors/Sub-contractors and their personnel involved in the programme/project/construction. Prime Contractors participating in the programme/project/construction shall be provided with the complete PSI, which shall be made binding through one of official NATO language. In case a Contractor/Sub-contractor will require only relevant provisions of the PSI, those provisions shall be provided in line with the respective need-to-know and made binding through one of official NATO languages and appropriate contractual language.

6-11. The following general principles shall be observed in connection with the security classification requirements of classified contract (prime and sub):

a. The assignment of a security classification to background information shall be the responsibility of the originator of the NCI; the classification of foreground information is a mutual responsibility of the participants in the programme/project/construction governed by the SCG.

b. Security classifications shall be applied only to those aspects of a programme/project/construction that must be protected, and the level of such classifications must be strictly related to the degree of protection required.

c. The security classification of a compilation of information from more than one source shall be co-ordinated with originators to determine the appropriate NATO security classification level and marking.

d. NCI related to the programme/project shall be downgraded or declassified as soon as appropriate subject to originator approval.

e. The originator will approve in writing any change of the classification level of background information. Changes to the classification of foreground information shall be co-ordinated among the participating originators.

6-12. Programme/project/construction SCG should be developed in close co-operation with industry participating in the programme/project. A ‘Security Classification Board’ may be established to assist in the preparation of SCG. Such Boards should be led by APO and comprised of appropriate representatives of the NSAs/DSAs of the participating nations and advised by the participating prime Contractor(s).

6-13. The initial assessment whether information should be classified, which was not previously identified for security classification in a programme/project/construction, may be made by the Contractor having system design responsibility. In such a case, the Contractor will recommend the APO to take appropriate security classification action. The security classification decisions will be codified in the programme/project/construction SCG.

6-14. In the absence of clearly defined SCG, any participant in the programme/project/ construction may forward a security classification proposal to the responsible APO regarding interim classifications. The APO shall review the proposed interim classification, consult with the NSAs/DSAs, and if agreed, update the programme/project/construction SCG.

6-15. The PSI, SCG and PMI shall be coordinated with the responsible NSA/DSA and issued and maintained by the APO. The PSI, SCG and PMI should be regularly reviewed and amended as necessary in consultation with the relevant NSAs/DSAs so that any security risks related to the programme/project/construction are identified and managed to ensure that the most appropriate degree of security is afforded throughout the programme/project/construction, including during disposal.

CHAPTER 7 – RELEASE OF NATO CLASSIFIED INFORMATION BY PROGRAMME/PROJECT PARTICIPANTS AND CONTRACTORS/SUB-CONTRACTORS

7-1. **SECURITY ARRANGEMENTS FOR THE RELEASE OF NCI TO NON-NATO ENTITIES.** Release of NCI related to NATO classified programme/project/construction within ACO shall always be based on a threat assessment and risk management of the relevant Delegated Authority. For the purpose of NATO classified programme/project/construction this authority may be delegated by the HQ commander to the head of APO.

7-2. If not programme/project/construction specific security marking (NATO/X), defining the programme/project/construction community is approved by the NAC, the NCI originated within ACO component, related to the programme/project/construction, shall always be marked as LIMITED and specific recipients shall be listed on the distribution list of the document. Release of NCI related to classified programme/project/construction to NNE without specifying the recipient should not be authorised.

7-3. Recipients of the NCI released shall be made aware that they are not authorised to further share received NCI originated within ACO component without written consent of the originator.

7-4. These release procedures shall be fully detailed by in the PSI.

7-5. Further advice and guidance on this matter can be obtained from the ACO SHAPE SEM J2X Security Policy Oversight (SPO) Section.

This page is intentionally left blank.

CHAPTER 8 – HANDLING OF NATO CLASSIFIED INFORMATION IN COMMUNICATION AND INFORMATION SYSTEMS

8-1. **General.** Only appropriately security accredited CIS (including stand-alone work stations) shall be used for the storing, processing or transmitting (called hereafter “handling") of NCI.

8-2. CIS used within national industrial facilities to handle NCI will be accredited by the respective national SAAs, or their delegated SAAs, ensuring that the NATO minimum security standards, as described in the policy on Security within the NATO and its supporting Directives on CIS Security, are met for the handling of programme/project/construction related NCI.

8-3. For security accreditation of CIS handling NCI, whose components are under different jurisdictional domains (e.g. different SAAs), all SAAs having a legitimate interest in the security of the CIS shall form a Security Accreditation Board.

8-4. The security accreditation of CIS handling information classified NR may be delegated to Contractors according to national laws and regulations. Where this delegation is exercised, the relevant NSAs/DSAs/SAAs will retain the responsibility for the protection of information classified NR handled by the Contractor and the right to inspect the security measures taken by the Contractors. In addition, the Contractor shall provide the Contracting Authority and, where appropriate, the security authority as established per Annex EE, with a statement of compliance certifying that the CIS handling information classified NR has been accredited in compliance with the NATO Security Policy and its supporting Directives on CIS Security as amended.

8-5. Interconnection of industrial facilities’ classified CIS to NATO CIS shall be jointly accredited by the respective national and ACO SAAs. The appropriate security arrangements shall be in place to ensure that the SAAs and the different CIS Providers of the interconnected CIS are bound by the requirement to protect NATO information.

8-6. Where required, the capability for handling NCI in CIS shall be reflected in the Facility Security Clearance Information Sheet (FSCIS) (connect Annex FF).

8-7. Enclosure F to C-M(2002)49-REV1, the “Primary Directive on CIS Security” (AC/35-D/2004), the “INFOSEC Management Directive for CIS” (AC/35-D/2005) and all relevant Technical and Implementation Directives on CIS Security (AC/322 documents) provide further policy and directions for the conformant implementation of CIS handling NCI.

8-8. For further guidance SHAPE SEM J2, J2X Information Assurance Section shall be consulted.

8-9. **Security Accreditation Process.** The security accreditation process shall determine the extent to which CIS Security measures are to be relied upon for the protection of NCI and system assets, during the process of establishing the security requirements. The security accreditation process shall determine that an adequate level of protection has been achieved, and is being maintained. The security accreditation process shall be carried out in accordance with the requirements of the INFOSEC Management Directive for CIS. Further advice and guidance can be obtained from SHAPE SEM J2, J2X Information Assurance Section.

8-10. **Security-Related Documentation.** Security-related documentation shall be established in accordance with the requirements of the INFOSEC Management Directive for CIS and the SAA requirements for a specific CIS. Security-related documentation shall be required throughout the system life cycle, from the planning stage until the disposal stage. The security-related documentation (e.g. System-specific Security Requirement Statements (SSRS) and Security Operating Procedures (SecOPs)) shall be developed in an iterative process throughout the system life cycle.

8-11. **Interconnection of CIS.** The NATO Security Policy and its supporting Directives on CIS Security require security measures to control the interconnection of CIS handling NCI. The supporting INFOSEC Management Directive for CIS sets out the security accreditation requirements and the supporting CIS Security Technical and Implementation Directives (AC/322 documents) set out the measures to be implemented. Further clarification should be sought from SHAPE, SEM J2X Information Assurance Section.

CHAPTER 9 – INTERNATIONAL VISIT CONTROL PROCEDURES

9-1. **Requirements and Procedures for Visits.** Procedures for visit requests are formalised in the standard Request for Visit (RFV) procedure as established at Annex S. Lead times for the handling of the requests are laid down in Annex LL.

This page is intentionally left blank.

CHAPTER 10 – INTERNATIONAL TRANSFER AND TRANSPORTATION OF NATO CLASSIFIED INFORMATION AND MATERIAL

10-1. **General.** The international transfer of NCI up to and including NS shall be as set out in this ACO Directive (Chapter 3, para 3-18 to 3-35). Electronic transmission of NCI shall be in accordance with the requirements of ACO CIS Security Directive AD 070-005. Information classified at the CTS level shall only be transmitted by ACO Courier Service. International hand carriage of CTS information and material is prohibited.

10-2. Information relating to contracts that is classified up to and including NS that cannot be transmitted by one of the foregoing methods may be transmitted by other means in accordance with the relevant provisions below. Further advice and guidance can be obtained from SHAPE SEM J2X Security Policy Oversight Section.

10-3. **Transfer by International Hand Carriage of NATO Classified Material at NC or NS Level.** When transfer through the channels specified in this Part III of this ACO Directive will result in an unacceptable delay that will adversely affect performance of the programme/project/construction, and when it has been verified that the material is not available at the intended destination, the procedure of personal hand carriage may be permitted, provided the following provisions are complied with:

a. The courier shall hold a PSC at appropriate level.

b. In exceptional circumstances, the APO may, with the previous coordination with the NSA/DSA of the receiving facility, consider issuing a Courier Certificate to an employee with the appropriate PSC who is assigned to the receiving facility, and to whose NATO nation the release of the classified material relating to the programme/project/construction has been authorised.

10-4. **Security Arrangements.** The transfer by hand carriage of NCI will comply with the provisions of this Directive (3-21). In addition, the information must have been authorised by the head of APO for release in conjunction with the project/programme/construction.

10-5. The courier shall be briefed by the APOSM before departure on all the security measures to be implemented and shall sign the Security Acknowledgment at Annex MM.

10-6. The courier shall be responsible for the safe custody of the NCI until such time that it has been handed over to the consignee’s FSO. In the event of a breach of security, the consignor's NSA/DSA may request the authorities in the country (i.e. a NATO nation or NNN with a Security Agreement/Arrangement with NATO or a NATO nation) in which the breach occurred to carry out an investigation, report their findings and take legal or other action as appropriate.

10-7. **Procedure.** When transfer by hand carriage of NCI originated within ACO component is permitted, the following minimum procedures shall apply:

a. The courier shall carry a Courier Certificate based on Annex NN, authorising the carriage of the package as identified on the document. The Courier Certificate shall be stamped and signed by the consignor’s APOSM. The stamp and the signature may be substituted by qualified digital signature.

b. A copy of the ‘Instructions for the Courier’ (Appendix 1 to Annex NN) shall be attached to the certificate.

c. The Courier Certificate shall be returned to the issuing APO immediately after completion of the journey. Any circumstances that occurred during the trip which raise security concerns shall be reported by the courier on the certificate.

10-8. If the courier is making multiple transfer by hand carriages of information classified NC and/or NS, then the ‘Multi-Travels Courier Certificate’ (Annex NN) shall include:

a. The couriers name and the destination countries. It will be stamped and signed by the consignor’s APOSM. The certificate shall not be valid for more than one year. The stamp and the signature may be substituted by qualified digital signature.

b. For each journey, a ‘Description of Consignment’ shall be signed by the consignor’s APOSM. This description will be returned to the issuing APO in order to assure accountability, or be kept available at the APO for monitoring purposes.

c. At the end of each journey, the courier will report any circumstances that occurred during the trip which raise security concerns on the 'Multi-Travels Courier Certificate’, or certify that no situation occurred that might have compromised the security of consignment during the journey, and sign the Note at the bottom. The declaration shall be witnessed by the APOSM.

10-9. The ACO component consignor's APOSM is responsible for instructing the courier in all of his duties and of the provisions of the ‘Instructions for the Courier’ (Appendix 1 to Annex NN) and a Security Acknowledgement (Annex MM) shall be signed.

10-10. If customs authorities of the NATO nation request to examine the consignment and inspection is unavoidable, the procedures detailed in the customs section below 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.

10-11. **Transfer of Information at the level NATO CONFIDENTIAL by Non-Security Cleared Commercial Courier Companies (CCC).** The following criteria shall be applied when consignments of ACO originated information classified NC is carried by non-security cleared CCCs:

a. The use of other transfer channels as described above is not feasible due to cause of urgency where the risk assessment indicates a manageable security risk.

b. The CCC provides courier services, and if required by national laws and regulations has concluded a framework arrangement with the NSA/DSA or with the ACO consignor’s APO which describes the specific obligations of CCC, include reporting obligations in case of suspected or actual breaches of security.

c. The CCC is located and registered in a NATO Nation and has established a protective security programme for handling valuable items with a signature service, including a record of continuous accountability on custody through either a signature and tally record, or an electronic tracking/tracing system.

d. The CCC shall provide the ACO consignor proof of delivery by obtained by the courier receipts against package numbers.

e. The CCC shall guarantee the transferred ACO consignment will be delivered to consignee prior to a specific time and date within a 48-hour defined period.

f. The CCC may charge a commissioner or Sub-contractor, which is located and registered in a NATO Nation and also meets the above requirements. However, the responsibility for fulfilling the above requirements must remain with the CCC.

10-12. **Transfer of Information Classified NATO CONFIDENTIAL or NATO SECRET by Transport as Freight.** The ACO consignor and the consignee of a consignment of information classified NC or NS to be transported as freight internationally shall jointly organise the transport arrangements. The ACO consignor shall submit a written International Transportation Plan (ITP) to its host NSA/DSA who, after consultation with the NSA/DSA of the consignee, will advise the ACO consignor whether the ITP is acceptable and/or of any changes that are required.

10-13. The host NSA/DSA of the ACO consignor will notify the NSA/DSA of any transited nation of the appropriate details of the transportation, including any cancellation thereof, with sufficient advance notice to enable them to provide the necessary security assistance.

10-14. When, in the opinion of the NSA/DSA concerned, a consignment at the level NC or NS is of such size and weight, or other circumstances render the standards defined in the NATO Security Policy or hand carriage impractical or unavailable, commercial carriers (CCa) may be used. The following procedures will be applied:

a. The CCa will hold an FSC if it is to store information classified NC or NS at its premises.

b. The CCa will deploy personnel that have been granted a PSC at a minimum level to the NCI being transported.

c. Prior to any international transfer by CCa, the NSAs/DSAs of the ACO consignor and of the consignee will agree on an ITP as described in Annex OO.

d. When an ITP is developed that will involve more than one international shipment of NCI, a Notice of Classified Consignment (Appendix 1 to Annex OO) 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.

10-15. **Transfer of Information Classified NATO CONFIDENTIAL or NATO SECRET by Transportation as Freight by Road.** The following minimum criteria shall be applied by CCa when consignments of ACO originated information classified NC or NS are transported by road:

a. When storage of classified consignments is required at the CCa’s facility, the CCa shall hold an FSC at the appropriate level.

b. Classified information shall be secured in vehicles or containers by a lock or padlock of a type currently approved by NSA/DSA concerned. Closed vans and cars will be sealed shall be used. If this is not physically possible, the consignment shall be encased to protect the classified aspects and prevent unauthorised 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 will hold a PSC at the level commensurate with the classification level of the information. At least one individual shall carry a 'Courier Certificate' based on Annex NN and assume responsibilities of the '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 security 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 information will be responsible for keeping the consignment under constant control.

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

10-16. **Transfer of Information Classified NATO CONFIDENTIAL or NATO SECRET by Transportation as Freight by Rail.** The following minimum criteria will be applied by CCa when consignments of information classified NC and NS are transported by rail :

a. Passenger accommodation shall be made available for appropriately cleared security guards or escorts who shall carry a Courier Certificate and assume responsibilities of a 'Courier' as described above.

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

10-17. 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.

10-18. **Transfer of Information Classified NATO CONFIDENTIAL or NATO SECRET by Transportation as Freight by Sea.** The following minimum standards shall be applied by CCa when consignments of ACO originated information classified NC or NS are sent by sea:

a. Where possible consignments should be carried in ships sailing under the flag of a NATO member nation. Ships sailing under the flag of a NNN, which represents a special security risk, 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 ACO consignor. However, when this is not possible, blocked-off stowage may be approved by the host NSA/DSA. 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 transferred information 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 NCI.

c. Stops at, or entering the territorial waters of, countries presenting special security risks shall normally be avoided; however, if unavoidable the security risk will be assessed by the NSAs/DSAs concerned in the light of the political environment, when they receive the ITP drawn up by the ACO 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 ACO consignor's host NSA/DSA has been obtained.

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

f. Deliveries to the port of embarkation and collection from the port of disembarkation shall 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 ACO consignor's host NSA/DSA and/or consignees NSA/DSA, as applicable. Where this is not possible, sufficient security guards shall be provided to keep the consignment under adequate and permanent supervision until collection is achieved.

10-19. **Transfer of Information Classified NATO CONFIDENTIAL or NATO SECRET by Transportation as Freight by Aircraft.** Preference shall be given to the use of military aircraft of a NATO Nation to transport information classified NC or NS. 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 the relevant NSA/DSA. Scandinavian Airlines System aircraft also may be used.

10-20. The following minimum standards shall be observed:

a. Every effort shall be made by the ACO consignor 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 an ACO component or host NSA/DSA's 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 by the consignee and his host NSA/DSA 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 shall 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 will remain in the aircraft. However, if the cargo compartment is to be opened, every effort will be made to ensure that the courier or other personnel

holding an appropriate PSC are available to ensure the protection of the consignment.

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 or of the Diplomatic mission supporting NATO in the country concerned.

f. Transportation over countries presenting special security risks should be avoided.

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

10-21. Companies that provide cargo handling services (such as freight forwarders) shall have an FSC and approved protection capability if a consignment with information classified NC or NS is to be stored at the facility.

10-22. **Security Principles Applicable to all Forms of Transportation.** Countries presenting special security risks shall be assessed by the NSAs/DSAs concerned in the light of the political environment, when they receive the transportation arrangements. Arrangements for consignments with NCI shall be stipulated for each ACO programme/project/construction by the relevant APO. However, such arrangements shall ensure that there is no likelihood of unauthorised access to NCI.

10-23. **Customs.** As a general rule, customs authorities shall be informed by the appropriate national authorities of impending consignments and shall be urged not to open consignments unless there is a pertinent reason for so doing, noting the need to maintain the need-to-know and the possibility to have the consignment repacked securely. If a consignment needs to be opened, this should be done in the presence of the courier. When access is no longer necessary it shall be repacked securely, and the customs authorities shall be requested to reseal it and endorse the shipping documents, confirming that it was opened by such authorities. To facilitate customs clearance, advantage should be taken of the Transport International Routier (TIR) for road shipments, Transport International Ferroviaire (TIF) for rail shipments, or other similar shipping arrangements.

10-24. Nothing in the previous paragraph or elsewhere in this section should be construed to abrogate any nation's rights of examination of any consignment.

10-25. **Acknowledgement.** The consignee shall acknowledge receipt of the consignment to the ACO component sender.

10-26. **Packaging.** Packaging of consignments shall be in compliance with this Directive. The registry ACO consigner's HQ is responsible for appropriate packaging. Under no circumstances shall the packaging reveal that the consignment contains NCI.

10-27. **Security Guards and Escorts.** Individuals fulfilling the duties of security guards may be civilian or military personnel and may be armed or unarmed depending on national practices and arrangements made between the APO and the NSAs/DSAs of the nations

affected by the transportation. Similarly, the nationality of such guards in any particular nation shall be subject to mutual agreement of the APO and the NSAs/DSAs and in accordance with Enclosure C to C-M(2002)49-REV1 and in the supporting Directive on Personnel Security (AC/35-D/2000).

10-28. In addition to the security guards, security escorts may be provided if the NSAs/DSAs concerned consider this desirable or as required under their national laws and regulations. These security escorts need not be security cleared unless otherwise required by national laws and regulations.

10-29. The security guard/escort shall be composed of an adequate number of personnel as to ensure regular tours of duty and rest. The number of guards/escorts on a consignment shall depend on the classification level of information, the method of transportation to be used, the estimated time in transit, and the quantity of material will also be considered. A reserve of personnel shall be provided to cater for emergencies.

10-30. It is the responsibility of the consignor's APO (and, where applicable, the consignee) to instruct security guards in their duties. In particular, the route and the security plan must be explained, and details given, where appropriate, of the authorities that security guards shall contact and other measures to be taken in the event of an emergency. Security guards shall also be given a copy of 'Notes for the Courier', and be required to sign the Security Acknowledgement.

10-31. The consignor's NSA/DSA may issue to the consignor APO sufficient authorisation documents so that they may be completed and issued to the security guards (connect Annex PP).

10-32. Both the authorisation documents and 'Instructions for the Courier' (Appendix 1 to Annex NN) shall be written in English and French; a copy in other languages may, in addition, be issued if this is deemed necessary or recommended by the NSA/DSA concerned.

10-33. **Transportation of Explosives, Propellants or Other Dangerous Substances.** If the consignment with the classified information contains explosives, propellants or other dangerous substances, the transfer across international borders is subject not only to the security and customs requirements, but also to mandatory international and national safety regulations. The ACO consignor is responsible for compliance with these regulations.

This page is intentionally left blank.

CHAPTER 11 – GLOSSARY AND ACRONYMS

Term	Definition
Background Information	Knowledge that has been generated by one of the participants outside of the collaborative programme/project/construction but which has been provided to the programme/project/construction. Only the originating participant needs to be consulted for authorising the release of that information to parties outside the programme/ project/construction.
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.
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) - NCI 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. NCI lost, even temporarily outside a Security Area shall be presumed compromised. NCI lost, even temporarily inside a Security Area, including documents which cannot be located at periodic inventories, shall be presumed compromised until investigation proves otherwise.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals or entities.
Consignee	The Contractor, facility, ACO component or other organisation receiving material from the consignor.

Term	Definition
Consignor	The ACO component represented by an APO, Contractor, facility or other organisation responsible for organising and dispatching material.
Contract	A legally enforceable agreement to provide goods or services.
NATO Classified Contract	Any contract issued by a NATO civil or military body (e.g. ACO component) or a NATO nation in support of a NATO funded or administered programme/project/construction that will require access to or generation of NCI.
Contractor	An industrial, commercial or other entity that seeks or agrees to provide goods or services.
Courier	A person officially assigned to hand-carry consignment containing information.
Designated Security Authority (DSA)	An authority responsible to the National Security Authority (NSA) of a NATO nation which is responsible for communicating to industry the national policy in all matters of NATO industrial security policy and for providing direction and assistance in its implementation. In some NATO nations, the function of a DSA may be carried out by the NSA or a DSA may delegate functions to other competent security authorities.
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.
Escorts	Armed or unarmed national police, military personnel, government personnel or other government designated personnel that facilitate the secure movement of information and materiel.

Term	Definition
Facility	An installation, plant, factory, laboratory, office, university or other educational Institution, or commercial undertaking, including any associated warehouses, storage areas, utilities and components which, when related by function and location, form an operating entity.
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 NCI up to a certain level.
Foreground Information	Foreground information is knowledge that has been generated in pursuance of a collaborative/cooperative programme/project/ construction. It is owned by all participants. To determine the releasability of foreground information approval of all owners is required.
Freight	Material carried by a vessel or vehicle, especially by a commercial carrier; cargo. Also – the commercial transportation of material.
Guards	Civilian (Government or participating Contractor employees) or military personnel who may be armed or unarmed. They may be assigned for security guard duties only or may combine security guard duties with other duties.
Industry	Organised economic activity concerned with manufacture, extraction and processing of raw materials, construction or output of a specific service.
Infraction	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 NCI, etc.).
Integrity	The property that information (including data, such as cipher text) has not been altered or destroyed in an unauthorised manner.

Term	Definition
International Visits	Visits made by individuals subject to one NSA/DSA or belonging to a NATO body (e.g. ACO component), to facilities or bodies subject to another NSA/DSA or to NATO, which will require, or may give rise to access to NCI or where, regardless of the level of classification involved, national legislation governing the establishment or body to be visited in support of NATO approved related activities requires that such visits shall be approved by the relevant NSA/DSA. ACO components and other NATO civil and military bodies fall within the security jurisdiction of NATO.
Major Programme/Project/ Construction	A programme, project or construction of major significance, normally involving more than two nations and security measures that extend beyond the normal basic requirements described in NATO Security Policy and this Directive.
Material	Material includes documents and also any items of machinery, equipment/components, weapons or tools, either manufactured or in the process of manufacture.
Nationals	Nationals includes “nationals of a Kingdom”, “citizens of a State”, and “Permanent Residents in Canada”. “Permanent Residents in Canada” are individuals who have gone through a national screening process including residency checks, criminal records and security checks, and who are going to obtain lawful permission to establish permanent residence in the nation.
National Security Authority (NSA)	An authority of a NATO nation which is responsible for the maintenance of security of NCI in national agencies and elements, military or civil, at home or abroad.
NATO	‘NATO’ denotes the North Atlantic Treaty Organisation and the bodies governed either by the Agreement on the status of the North Atlantic Treaty Organisation, National Representatives and International Staff, signed in Ottawa on 20th September, 1951 or by the Protocol on the status of International Military Headquarters set up pursuant to the North Atlantic Treaty, signed in Paris on 28th August, 1952.

Term	Definition
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 Programme/Project/ Construction	A Council approved programme/project/construction that is administered by a NATO agency/office (e.g. ACO Programme Office (APO)) under NATO regulations.
NATO Programme/Project/ Construction Agency/Office (NPA/NPO or APO for ACO led activity)	The executive body for the administration of a NATO programme/project/construction.
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.
Negotiations	The term encompasses all aspects of awarding a contract or sub-contract from the initial “notification of intention to call for bids” to the final decision to let a contract or sub-contract.
Originator	The nation or organisation under whose authority information has been produced or introduced into NATO.
Personnel Security Clearance (PSC)	A PSC is a positive determination by which an NSA/DSA formally recognises the individual’s eligibility to have access to information classified NC and above taking into account their loyalty, trustworthiness and reliability.
Personnel Security Clearance Confirmation (PSCC)	An approved format used by NSAs/DSAs to confirm the level and validity of a PSC.
Prime Contract	The initial contract led by a NATO Project Management/Agency/ Office (e.g. APO) for a programme/project/construction.

Term	Definition
Prime Contractor	An industrial, commercial or other entity of a NATO nation which has contracted with an APO to perform a service, or manufacture a product, in the framework of a NATO project/construction, and which, in turn, may subcontract with potential Sub-contractors as approved.
Programme/Project/ Construction Security Classification Guide	Part of the program/project/construction 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 lifecycle, and the elements of information may be re-classified or downgraded.
Programme/Project/ Construction Security Instruction (PSI)	A compilation of security regulations/procedures, based upon NATO Security Policy followed by supporting directives and this ACO Directive, which are applied to a specific project/programme/construction in order to standardise security procedures. The PSI may constitute an Annex to the prime contract, and may be revised throughout the programme lifecycle. For sub-contracts let within the programme, the PSI constitutes the basis for the SAL.
Registered Mail	A mail service that enables possibility to track the shipment from the sender to the recipient and allows the sender a proof of delivery.
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.
Risk management	A systematic approach to determining which security counter- measures are required to protect information and supporting services and resources, based upon an assessment of the threats and vulnerabilities. Risk management involves planning, organising, directing and controlling resources to ensure that the risk remains within acceptable bounds.
Security Aspects Letter (SAL)	A document, issued by the appropriate authority, as part of any NATO classified contract or sub-contract, other than Major Programmes/Projects/Constructions, identifying the security requirements or those elements thereof requiring security protection.

Term	Definition
Security Breach	A Security Breach is an act of omission, deliberate or accidental contrary to NATO Security Policy and supporting directives, that may result in actual or possible compromise of NCI or supporting services and resources including but not limited to: NCI lost; NCI subject to access by personnel without the correct level of PSC and/or without a need-to-know; NCI stored in an unescorted cabinet or one not approved for the level of classified information held; NCI left in unsecured area where unclears persons have unescorted access; NCI cannot be found at the expected location; NCI transferred by method not approved by this ACO Directive; NCI handled on a system, which is not appropriately accredited for the level of NATO security classification; NCI has been subject to unauthorised modification; NCI is deliberately under-classified; NCI has been destroyed in an unauthorised manner; or For CIS, there is denial of service.
Security Classification Check List (SCCL)	Part of a security aspect letter (SAL) which describes the elements of a contract that are classified specifying the security classification levels. In case of contracts let within a programme/project, such elements of information derive from the PSIs issued for that programme.
Sub-contract	A contract entered into by a prime Contractor with another Contractor (i.e. the Sub-contractor) for a provision of goods or services.
Sub-contractor	A Contractor to whom a prime Contractor lets a sub-contract.
Threat	The potential for compromise, loss or theft of NCI 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.

Term	Definition
Transportation by freight	Transportation of a consignment of such size and weight which makes the application of the respective standards defined in this ACO Directive or hand carriage impractical.
Vulnerability	A weakness, an attribute, or lack of control that would allow or facilitate a threat actuation against NCI or supporting services and resources.

PART VIII

ACO SECURITY FORMS

All forms can be found in the Enterprise Document Management System.

This page is intentionally left blank.

ANNEX A TO
AD 070-001
DATED 22 DEC 21

PHYSICAL PROTECTION / MINIMUM STANDARDS

1. **Introduction.** This Annex, which supplements Part II Chapter 1 of this Directive, sets out the minimum standards for the physical protection of Secure Areas when such protection is required to augment security guards or patrols. When standards are not explicit, the relevant standard of the host nation of an organisation shall be taken as the standard unless a combination of national and NATO standards would lead to an incongruous solution. In such a case, ACO J2X at SHAPE will advise on standards to be adopted.

2. **PHYSICAL BARRIER.** Perimeter barriers defining the physical confines of security areas or installations, are used to:

a. Restrict or impede access to the enclosed area.

b. Create a physical and psychological deterrent to accidental entry into an area.

c. Deter and deny unauthorised entry by overt or covert means.

d. Delay intrusion into an area to give time for reaction by a guard force; perimeter fences only delay a determined intruder for a very short time and should be supplemented by Intrusion Detection Systems (IDS), Closed-Circuit Television (CCTV), security lighting and/or guards.

e. Facilitate identification and control procedures by channelling the flow of authorised persons and vehicles through fixed entry points.

3. **Positive barriers** are required for the entire perimeter of security areas. Specific types of barriers cannot be pre-designated for all situations; they may, however, incorporate the following functions:

a. Provision at points of entry and exit for control of entry preferably by either pass exchange or examination.

b. Be constructed as opaque barriers to preclude visual compromise by unauthorised personnel in those instances when necessary.

4. **Perimeter fencing** should be a minimum of 50 x 50mm mesh chain link with a core diameter of 3mm. The chain link fencing should be at least 2.15m high supplemented by a top guard (a “Tee” member supporting coils of barbed tape or an overhang of at least three strands of barbed or saber wire facing outward and upward at an angle of 45°). The chain link should be galvanised or plastic coated and the barbed wire galvanised to inhibit corrosion. Tension wires should be installed along the top, centre and bottom of the fence fabric. The under fence gap should not exceed 50mm and the fence should be anchored at the bottom with steel spikes 1m in length separated by no more than 1m to prevent it being lifted; where soft soil conditions exist, the fence base should be anchored in concrete or asphalt curbs. Fence posts shall be of concrete or corrosion protected material. Gates should be constructed to the same standard as the fence of which they

form a part; ground surfaces under gates should be paved. The fence design should be in straight sections to permit an unobstructed field of vision and whenever possible a clearing of 25m should be maintained on both sides of the perimeter barrier.

5. **Walls of Buildings.** If used to provide the protection barrier, all windows and openings less than 5.5m above uncontrolled ground[19], roofs, ledges or drainpipes shall be protected by mild steel bars in a welded steel frame, bolted securely to the structure on the inside of the window or opening. The bars shall be 25mm thick (minimum 20mm) at 150mm centres and shall be supported by horizontal flats 45 x 6mm, at 200mm (maximum 500mm) centres. Alternatively, approved security glass that is toughened to provide commensurate protection in lieu of bars, may be used. Such glass shall be opaque or darkened to prevent overlooking. Local conditions i.e. frequency of patrols may require such openings to be alarmed.

6. **Gates and Perimeter Entrances.** Active vehicle and pedestrian points to an external perimeter or an internal secure area shall be limited to the minimum number required for the safe and efficient operation of the installation. Such access points shall, at minimum, be to the same security standard as the perimeter fencing and shall include a combination of technical and physical security measures, such as CCTV, Perimeter Intrusion Detection Systems (PIDS) and guard patrols.

7. **Perimeter Security Lighting.** Shall provide the illumination necessary for effective surveillance either directly by security personnel or indirectly through a CCTV system. Alongside CCTV, security lighting offers a high degree of deterrence to a potential intruder. The standard of lighting shall meet the minimum requirement of the CCTV and shall be installed in a manner which is appropriate to the site conditions, such as terrain and identified vulnerabilities.

8. **Terrain or Climate.** When conditions are such that perimeter fences are frequently damaged or are ineffective, alternative forms of protection such as alarm systems or continuous surveillance shall be used.

9. **The outer perimeter doors** of Class I or Class II areas shall be of solid wood or steel plated, free of abrasions to detect attempts of surreptitious entry. Hinges should be located on the interior, or hinge-pins should be brazed, or welded to prevent unauthorised removal of the door. The frame and fixing shall be at least as strong as the door itself and shall incorporate dog bolts (lag bolts). The walls, in which perimeter doors are set, including overhead door transoms, should not be significantly weaker than the doors themselves. No glass, other than reinforced glass to give the same protection as the fabric of the building, shall be used in security doors. Perimeter doors to Class II Security Areas shall be equipped with a Group B lock. Those to a Class I Security Area shall be fitted with built-in Group A changeable combination lock. Drill resistant hardened steel plates shall be installed between the lock-case and the door. An IDS shall be fitted to each entry door to a Class I Security Area, which shall also be monitored by CCTV.

10. **Interior doors** to offices within a Class I or Class II Security Area do not form part of the perimeter; therefore they may be of normal internal door construction.

11. **Electronic Control of Entry Systems.** Electronic cipher locks and magnetic key

[19] Ground which physical access is not controlled by perimeter barriers (see Para. 2 - 1 - A - 2).

card operated systems are designated "control of entry systems" only. They may be installed to augment the security guard force in their control of entry duties and may be used to allow unmanned control of entry points provided the guard can monitor and control the entry point(s) by remote means; under no circumstances are they approved as the sole means for the protection of classified information. Systems shall be installed in such a manner to prevent deliberate bypassing and may only be installed in Class I or II Security Areas or sensitive zones providing that they are continually under the central control and surveillance of the security force that shall have a capability to respond to incidents.

12. **Intrusion Detection Systems (IDS).** Intrusion detection alarms may be employed to augment the basic security elements. Alarms possess no inherent capability to provide security. However, when they are integrated in a physical security system, to include an alarm verification system such as CCTV, they increase its effectiveness and economise on other security resources.

13. **Closed Circuit Television (CCTV).** The use of CCTV is a valuable aid to security guards in verifying incidents and IDS affixed to perimeters; however, the effectiveness of CCTV depends on the selection and installation of suitable equipment, as well as a monitoring and response capability. Expert advice shall be sought when establishing the optimal CCTV design such as technical characteristics, camera installation locations, system redundancy, recording and control centre monitoring. Care shall be taken to ensure that audio and visual data captured by CCTV does not put NCI at risk of overlooking.

14. **Security Plan.** The security plan must be tailored to the security needs of each installation and, therefore, no single alarm system or device will be appropriate for all security systems.

15. Correct functioning of all alarm systems shall be verified daily by security personnel. There should be frequent technical tests, and a maintenance contract to ensure continuous serviceability.

16. Only alarm systems, which cannot be easily neutralised or compromised, shall be considered for security application. Alarm systems shall be installed to prevent deliberate bypassing of the system. A central security control shall be established to monitor and direct reaction to any alarm.

17. Systems must have been examined by experts and have been officially licensed or certified by NATO member nations for the protection of areas, rooms or containers used to store documents classified NATO CONFIDENTIAL and above. Further detailed guidance may be found in the ACO SOP on Technical Security produced by ACCI. Alarm systems in Technically Secure Areas (TSAs) must comply with the provisions of this SOP.

ANNEX B TO
AD 070-001
DATED 22 DEC 21

STORAGE OF NATO CLASSIFIED MATERIAL

1. **Introduction.** This Annex, which supplements Part II, Chapter 1 of this Directive, sets out the minimum standards for storage of NATO classified material and the requirements for the control of security keys and combination settings. Whilst member nations are responsible for certifying security containers (including vaults/strong-rooms) and locks, knowledge of appropriate criteria will assist security staff to ensure compliance. ACO J2X should be consulted and will advise on any case where deviation from these standards is being proposed.

2. **Security Containers.** Each member nation will establish its own criteria for setting the security specifications of security containers, for evaluating those proposed for procurement and for methods and procedures for testing and certifying security containers for the storage of NCI. All containers must offer protection against both surreptitious and forced entry and, clearly, the environment in which a security container stands is also relevant. External security measures should prevent unauthorised access and will be a major factor in determining the time delay factor that must be built into each category of container. Therefore, the minimum standards of security containers shall take into account:

a. The level of classification of the content.

b. The security value of the container and associated lock.

c. The combination of ancillary measures protecting the environment of each container.

d. The threat to security in the area in which the information is held.

3. **The Following General Specifications Apply**

a. The formation and joining of all the containers parts and the final assembly and manufacturing tolerances shall provide the required structural strength and ensure continued compliance with the requirements specified for each type of container.

b. The finished container shall be free of any defects, which might affect serviceability and appearance. Metal parts shall be free from rust, scale and other imperfections. Hardened steel shall be drill resistant and of sufficient thickness to offer a delay factor in forced entry opening consistent with the class of the container. All exterior and interior surfaces shall be properly finished and rust proof.

c. The container shall be fitted with a built-in three position changeable combination lock. It shall be impossible to secure the lock and allow any closed drawer or doors of the container/safe to remain unlocked. A safe shall have a positive dead bolt mechanism and associated linkage securely engaging with the lock in the locked position. Electronic combination locks may be used for security containers.

d. The manufacturer shall provide sample containers and locks for testing by the purchaser. The purchaser will also be furnished detailed view drawings of moving parts and mountings, to include locking mechanisms.

e. The container base shall be of the same dimension as the top. Weight for the heaviest container should not exceed 11 kilos per square centimetre of the base area. Basic storage of containers will accommodate letter or legal size files in file type drawers. Alternate storage may include optional shelves instead of drawers.

4. **Strong-Rooms and Vaults.** The following are the minimum criteria to be applied to strong-rooms and vaults within ACO.

a. **Strong-Rooms.** A strong-room is a burglar-resistant room with walls of masonry, concrete, brick or similar heavy construction, with a resistance equivalent to 15cm of concrete or concrete block or of metal of equivalent strength. The use of external walls should be avoided where possible; ideally it should be possible to inspect walls, floors and ceilings. Windows shall be protected by security approved toughened glass or by steel bars at least 2cm in diameter embedded in concrete and positioned not more than 15cm apart. (However, if the area is above 5.5m and proper perimeter security of the building including anti-climbing measures is maintained, the windows may be secured by heavy-gauge wire of at least 0.30cm in diameter secured to the wall so that the wire must be cut to permit entry). Windows shall be covered with opaque material. The doorframe and the door to the strong-room shall be steel or steel-covered and equipped with a built-in, changeable Group A combination lock (see Para 5. a.). The hinges of the door shall be located on the inside or shall be brazed or welded to prevent unauthorised entry. A back plate of metal concealing the lock and linkage shall be securely fastened to the door in such a manner as to preclude easy removal; however, a removable inspection plate shall be attached to the back plate. Ventilation systems shall be protected against unauthorised access or the introduction of any solid material. The floors and ceilings shall be of equivalent construction to the walls, to afford a comparable degree of difficulty to any illegal entry attempts. Additional security may be obtained by use of alarm systems activated by penetration of walls, floors, ceilings and openings or motion within the room.

b. **Vaults.** A vault shall meet the same specifications as a strong room except that, apart from the door, there shall be no openings in excess of 500 sq. cm (77 sq. ins.) and any such openings shall be protected in a manner, which prohibits the passage of any solid material. The vault door, which should be of strong steel and equipped with a changeable Group A combination lock (see Para 5. a.), shall meet the specifications laid down by a NATO member nation for the storage of documents or material classified up to and including COSMIC TOP SECRET.

SECURITY LOCKING DEVICES

5. **Categories of Security Locks.** Locking devices may be grouped as follows:

a. **Group A Lock.** A Group A security lock is one which a NATO member nation has certified as suitable for the protection of material classified COSMIC TOP SECRET. The combination change feature shall be of the key type from the rear of the case. Such locks incorporate advanced design features against expert manipulation not found in conventional designs and afford resistance to

unauthorised opening by professional manipulation for at least 20 man hours. In particular, there should be protection against radiological attack (x-rays). The lock will contain a mechanical means for securing the locking bolt in the locked position when entry is attempted to the interior of the lock case by punch methods from the front.

b. **Group B Lock.** A Group B lock is one, which a NATO member nation has certified as suitable for the protection of material classified NATO SECRET. A key or other required device for changing the combination shall be provided with each lock. It will be resistant to expert manipulation without having the advanced design features of a Group A lock.

c. **Group C Lock.** Certified as suitable for office furniture and security containers accepted for storage of NATO RESTRICTED information.

COMBINATION PADLOCKS

6. Combination padlocks should provide a high degree of security against surreptitious or forceful opening. The mechanism should be positive in its movement and should not transmit by feel, sight or sound, indications of the combination settings either with or without tension or pressure on the shackle.

7. The padlock shall be able to withstand a direct tension between case and shackle of at least 250 kilos without opening or impairment for subsequent use. The arrangement and fit of parts should be such that it will not be possible to insert a probing device to release arms, dogs or bolts, or to discover the locations of wheel gates or their positions in relating to each other or to the drive wheel. The mechanism should be so designed and constructed that jarring or impact could not open the lock. The case of the padlock should be so constructed that it cannot be opened without mutilation such as would make impossible the replacement of parts without discernible evidence of mutilation.

8. The outside dimension across the shackle is not to be more than 5 cm and the space under the shackle shall be of sufficient size to fasten around a 2 cm diameter bar. The diameter to the shackle is not to be more than 1 cm. The case dimension should not exceed 7 cm in height and width and 3 cm in depth.

9. The case, cover, and dial should be of bronze, brass or zinc alloy. The combination setting shield should be of casehardened steel. All movable functional parts affecting the setting of the combination should be of non-magnetic material and not more corrodible than brass or bronze. The drive wheel or cam and other internal parts similarly subjected to wear with the exception of the locking bolt shall be of brass, bronze or zinc alloy. The shackle locking arms, dogs or bolts shall be of brass, bronze or steel and the shackle shall be of casehardened steel.

10. The locking bolt shall be guarded by not less than three combination wheels and a driving wheel or cam. The combination wheels shall be readily changeable and shall provide at least 100,000 combinations. The mechanism shall preclude the changing of the combination without knowledge of the existing dial settings. The dial tolerance for opening is not to exceed one dial division or number, from either side of any true dial setting. The locks shall contain a device, which on locking or pushing home the shackle, disperses, or scrambles the wheels to upset the combination in an indeterminable manner. Movement of the dial through one-third resolution shall securely lock the shackle so that dialling the

combination will be required for re-opening. The lock mechanism is not to permit the shackle to be locked out in the open position. The shackle is not to automatically spring out to the open position when the padlock is unlocked, but require a pull to place in the open position. A key or other required device for changing the combination shall be provided with each padlock.

11. **Locking Bars.** If a rigid "T" cross-section locking bar is not fitted, a recommended locking bar for use on metal filing cabinets shall conform with the following:

a. Material stock shall be of cold rolled steel not less than 3mm in thickness to provide necessary rigidity.

b. Maximum clearance between the bar and cabinet drawer face is not to exceed 5mm. This feature is necessary in order to eliminate possible document removal from a drawer through the small aperture, which would result from excessive clearance.

c. Installation of the three bar guide brackets shall be accomplished by brazing. Where the thinness of the cabinet metal precludes it, the brackets shall be installed with steel rivets sufficiently turned to prevent any movement of the brackets.

d. The recommendations in the preceding sub-paragraphs do not preclude the use of containers with locking bars and hasps of different design so long as the construction affords the same degree of security.

COMBINATION LOCKS

12. In general, combination locks are designed for attachment on security containers and doors of strong rooms and vaults for the storage of NCI and are much more secure than combination padlocks. The primary purpose of each type of lock shall provide a means of securing the associated bolt and linkage or locking bar mechanism against unauthorised opening. Combination locks may or may not have built-in protection against entry by force. The design and accuracy of construction are primarily to guard against unauthorised opening of the combination lock by sense of sight, touch or hearing. Combination locks are generally of hand change or key change types. The latter avoid opening of the lock cases and handling of internal parts by inexperienced personnel.

13. The lock mechanism shall be enclosed in a metal case of sufficient strength to withstand normal rough usage without distortion.

14. The working mechanism is to be of not less than three combination wheels plus a driving wheel or cam. A three-tumbler (combination wheels) lock should not open if more than one dial graduation is exceeded on either side of the proper number for each tumbler wheel. A four- tumbler lock should not open if more than 1-1.5 dial graduations are exceeded on either side of the proper number for each tumbler wheel. The dial shall have a minimum of 100 graduations.

15. Electronic combination locks may be used for security containers. Electronic combination locks are required to offer equivalent security compared to mechanical equivalent combination locks.

16. **Protection of Locks.** The following measures shall be taken to protect locks

against tampering:

a. To be secured during transit and storage.

b. The locking mechanism shall be inspected after transit and at prescribed intervals.

c. To be installed and maintained by cleared personnel.

d. Access to the back of the lock to be denied to unauthorised persons during normal use.

17. **Protection of Combinations.** A combination setting requires the same level of security protection as is given to the most highly classified material to which it gives access. The settings shall be protected as follows:

a. Committed to memory and are not to be written down by the user; but see sub- paragraph 17 c. below. In choosing combination settings, numbers that are too close together or simple numeric combinations should be avoided.

b. Unique settings shall be used for individual containers; however, exceptionally, the same combination may be used for multiple containers serving a common user group, by example Registries.

c. A record of combination settings for emergency use shall be recorded on ACO Form 86 (see Part VIII, ACO Form 86) and held in sealed opaque envelopes as directed by the Headquarters Security Officer.

d. The combination settings shall be classified at the same level as the information they protect and handled accordingly.

e. Combination settings shall be changed as follows:

(1) On receipt of the lock or equipment to which it is fitted from the manufacturers and after any maintenance on the lock.

(2) On transfer of any person who has knowledge of the combination.

(3) On compromise or possible compromise of the combination setting.

(4) At intervals, preferably every 6 months, but at a maximum interval not exceeding 12 months.

f. Entirely new combinations shall be used each time they are changed. To avoid "lockouts" or other malfunctions, the new combination can be set by the user under the direction of specialists or locksmiths without the latter becoming aware of the new combination.

18. **Security Keys.** Security keys shall be protected as follows:

a. Issued against signature and only to authorised personnel.

b. A register of all keys, including spares, together with a record of the related

lock or container number, shall be maintained.

c. Security keys are never to be removed from a place of duty except keys to briefcases or pouches, which are never to leave the possession of the custodian, and are not to be attached to the briefcase or pouch when in transit. Spare keys shall be placed in sealed envelopes marked with the appropriate security classification and held centrally by the appropriate security officer in an appropriate security container.

d. Comparable protection can also be achieved by combination padlocks provided that they are safeguarded against manipulation by unauthorised persons through access to the back of the padlock or through exchange.

PROTECTION OF COPYING AND TELEFAX MACHINES

19. Copying and fax machines shall be afforded the necessary protection to ensure that only authorised persons use them. As commercially serviced/leased copy machines contain electronic components capable of storing information, copy machines shall not be used to reproduce any information classified NATO SECRET or COSMIC TOP SECRET/ATOMAL.

20. The array of media available for processing information throughout ACO has created a need to be able to readily identify the users, the suitability of certain office equipment for processing classified information and the level that may be processed on this equipment. Conversely, there is also a need to identify those machines that are unsuitable for such purposes. All electronic information processing equipment including photocopiers, fax machines, computers, etc., shall be marked with an approved label indicating their suitability/unsuitability for processing classified information.

ANNEX C TO
AD 070-001
DATED 22 DEC 21

TECHNICAL SECURITY

1. **Definition.** Technical Surveillance Countermeasures (TSCM) are the techniques used to prevent, or to detect and neutralise, hostile intelligence efforts to obtain classified or sensitive information through the introduction of a clandestine monitoring device, or the exploitation of weaknesses in sensitive work areas. TSCM procedures are conducted by the ACCI who are responsible for:

a. Providing investigative support and services as described in this Chapter.

b. Recommending to the command and to ACO SHAPE J2X what actions should be taken in cases of non-compliance with this Chapter.

c. Staffing the ACO SOP on Technical Security.

In the event that ACCI is not available to provide these services, ACO organisations may seek approval from ACO SHAPE J2X to use the services of host country security organisations.

2. **TCSM Programme.** Activities include two general categories:

a. **TSCM Investigations.** Technically-oriented Counter-Intelligence investigations. The primary objective is to detect and neutralise espionage efforts. Secondary objectives shall detect and rectify technical security hazards, and to enhance physical security. TSCM investigations are described in Para. 4.

b. **TSCM Services.** Preventive activities in support of the command's security programme. The primary objective is to assist the security officer to "harden" a facility to preclude the installation of clandestine listening devices, and to exclude equipment prone to standoff exploitation by hostile intelligence services. Adopting strict physical and technical security measures hardens a facility. TSCM Services are described in Para. 5.

3. **Requests for Technical Surveillance Countermeasures investigations**

a. **Requesting Support.** All requests for TSCM support shall be submitted to the HQSO for approval. The HQSO will forward requests to ACCI. ACO Form 165(R) (see Part VIII, ACO Form 165) should be used. Telephone requests will automatically compromise the planned investigation, which will then be cancelled or postponed. Requests for TSCM Investigations involving clandestine listening devices shall be classified NATO CONFIDENTIAL. All other requests shall be classified according to content.

b. **Validating and Scheduling.** ACCI will validate all TSCM support requests based on priorities set by the type of TSCM Investigation described in Para. 4.

4. **TSCM Investigations.** There are three types of TSCM Investigations:

a. **Penetration Investigation.** An investigation of a technical monitoring system. If a suspected or confirmed incident of technical surveillance occurs, the

following immediate actions shall be taken:

(1) **Stop Classified Discussions.** Cease all classified activity immediately and as discreetly as possible. Do not voice the discovery within the immediate area, which includes the suspect room and all adjacent rooms. Secure the area to preclude any attempts to remove or modify the installed device(s). Conduct normal unclassified activity within the areas, limit access to the minimum, entitled personnel and maintain an access list.

(2) **Notify.** The facility manager, the Security Authority and the Commander, ACCI shall be notified immediately of the suspected technical surveillance device. This information will not be released to other persons until such time as the Commander and the ACCI element have been consulted.

(3) **Do Not Tamper.** Only TSCM personnel from the ACCI element are authorised to remove and confiscate any suspected surveillance devices from a room/area.

b. **TSCM Investigation of an Area.** A thorough physical, electronic (to include but not limited to computer and or telephony networks, but at a minimum, a through technical evaluation of electrical power and telecommunication equipment within the area), and visual examination of an area by TSCM personnel to detect technical monitoring devices and technical security vulnerabilities. Areas for TSCM investigation include (but are not limited to):

(1) **TSAs.** An initial TSCM Investigation is required, and serves as the basis for command certification of new TSAs. This shall be repeated every 18 months and after any event, which may have compromised the security integrity of the room (construction, etc.).

(2) **Security Areas.** A TSCM Investigation may be conducted in a security area determined to be a lucrative target for hostile intelligence service technical exploitation where there is a high level of threat.

c. **TSCM Investigation of an Event.** An investigation that is limited in scope and designed to augment other security measures during sensitive, time specific events occurring either on or off ACO-owned facilities. Sensitive events include (but are not limited to):

(1) **Conferences/Briefings.** When facilities other than TSAs must be used for conferences/briefings which discuss COSMIC TOP SECRET information, Special Access material or critically sensitive information, a TSCM investigation should be requested. Use of facilities that do not have continuous security controls is not permitted.

(2) **Military Exercises.** TSCM investigative support should be requested for TSAs established during tactical deployments/military exercises.

(3) **Travel Support.** When current threat assessments dictate, TSCM investigative support is available to complement other information/communications security measures necessary to protect

sensitive/classified NATO information during official travel.

5. **TCSM Advice and Assistance.** Advice and assistance can be provided by TSCM personnel to command security officials at any time during the life cycle of a secure area from preconstruction planning to final closure.

a. **Preconstruction Advice and Assistance.** Conducted prior to and during construction or renovation of a facility to ensure that appropriate physical and technical security safeguards are included. This assistance can also be requested for any security area, however, is not mandatory for TSAs.

b. **Ongoing Advice and Assistance.** After the facility is operational, TSCM support is still available to assist security officers and commanders resolve security questions of a technical nature.

6. **Counter Surreptitious Entry.** This technical service is designed to assist command security personnel to evaluate the physical security posture of all areas including TSAs. Specific services include advice concerning locks and locking devices and Technical evaluations with a focus on prevention and detection of surreptitious entry into secure areas.

7. **Technical Threats Briefings.** Awareness briefings may be provided by TSCM personnel. They may be designed to complement a command security education programme or tailored to address a specific need or problem.

8. **Entrance and Exit Briefings.** These briefings are a mandatory part of all TSCM investigations of an area.

a. **Entrance Briefings.** The TSCM Team Chief will provide the command with an initial briefing, which will define the scope of the investigative support to be performed, the sensitivity of the service and answer questions posed by command personnel. All key personnel identified by the HQSO must attend this briefing. TSA Facility Managers will bring the TSA Facility Profile to the Entrance Briefing.

b. **Exit Briefings.** The TSCM Team Chief will provide the command with a final briefing after the TSCM investigative service is completed. This briefing will detail the result of the TSCM investigative support and the command actions required to correct any deficiencies.

9. **Reports.** Following TSCM investigations and advice and Assistance services, the supporting ACCI element will render a report within ten working days describing the conduct of the investigation, its results or findings or security deficiencies and recommendations for remedial measures to be taken by the supported command.

10. **Termination of Service.** Occupants of the area will be instructed not to make comments that could indicate to hostile intelligence that a TSCM investigation is to be conducted or is in progress. Should this occur, the investigation may be terminated immediately on the authority of the TSCM Team Chief, an exit briefing conducted, and the service rescheduled. A report will be rendered stating the reasons the investigation was terminated.

11. **Command After Action.** Within 30 calendar days of receipt of the TSCM

Investigative Report, recipient Commanders shall report to ACO SHAPE J2X in one of three ways:

a. Confirmation that any deficiencies have been corrected and seeking re-certification of the TSA, or

b. Providing an estimate of timescale for completion of corrective action and seeking a temporary waiver for continuing use as a TSA (temporary re-certification).

c. Confirmation that the reported weaknesses cannot be corrected (e.g. building design) and seeking a permanent waiver. Such waivers will only be granted when the deficiency is of a minor nature, which will not seriously compromise the integrity of the TSA.

12. **General.** SOP on Technical Security is the only authorised supplement on technical security requirements outlined in this Directive. ACCI TSCM personnel shall be granted unescorted access to the facility under inspection. Any special access or clearance requirements will be specified at the time of the request for service to ensure proper clearances and accesses are passed to the appropriate security agency prior to the scheduled TSCM Investigative service date.

13. **TCSM Equipment.** HQSOs shall ensure TSCM equipment will be admitted to sensitive areas without delay or question under any circumstances, as long as the personnel operating the equipment are certified as having the appropriate level of security clearance. No person is authorised access to the equipment or may observe the techniques unless he is a member of the inspection team and has a "need to know".

TECHNICALLY SECURE AREAS MINIMUM STANDARDS OF SECURITY

14. **Introduction.** This section of the Annex sets out the specific security requirements for Technically Secure Areas (TSAs), which require enhanced technical and physical security due to the frequent discussion and/or processing of COSMIC TOP SECRET or special access material. The applicable Commander designates TSAs. Advice concerning areas used for occasional discussion or processing of CTS material should be requested from the HQSO, who will consult ACCI.

SPECIFIC REQUIREMENTS

15. **Telephone Security.** Telephones are one of the weakest links in the technical security arena. Telephones shall not normally be installed in TSAs unless unavoidable. In this case, telephone systems/equipment must fulfil the following minimum security requirements:

a. Telephone systems within the TSA will incorporate a positive disconnect device or, the telephone shall be physically disconnected when classified discussions take place.

b. In new installations, telephones lines will enter the TSA at a single point. If there is more than one instrument, lines will be terminated at a distribution block and identified as to use by specific name or (telephone) number.

c. All excess wiring will be removed or bound together and grounded.

d. Speakerphones will not be used in TSAs.

16. **Mobile Telephones.** No mobile communication device, (whether official, registered or privately owned), except NATO approved secure mobile communication devices operating in the secure mode (after the initial, non-secure “handshake”), shall be introduced into Class 1 Security Areas, TSAs or any other areas where CTS or Special Category information is discussed.

17. **Networks.** Facilities containing network information systems will require network analysis as part of the TSCM investigation. TSCM teams shall assess computer networks at the basic, physical, and logical level to detect unauthorised users and devices operating within NATO networks. TSCM analysis of networks is not intended to replace other network security processes. Instead, TSCM efforts shall complement other aspects of information assurance.

18. **Intercoms and Intercommunications Equipment.** These systems will not be used in TSAs unless approved in writing by the responsible command authority as essential to operations. If approved and installed the following guidelines must be met.

a. No station or wiring will be located outside of the TSA and wiring will be installed to permit visual observation.

b. Systems will not use established power lines or any radio frequency means as a transmission link between stations.

c. Each intercom instrument will be clearly marked "NO CLASSIFIED MATTER WILL BE DISCUSSED OVER THIS INSTRUMENT”.

d. Intercommunication systems will be designed to indicate when a station is in the active mode.

e. When, for safety reasons, an intercommunications system is mandated to notify personnel of emergencies, the system will be unidirectional. A buffer amplifier, which restricts audio transmissions out of the facility, will be included at the point the transmission lines breach the perimeter of the facility.

19. **False Ceilings, Walls and Floors.** False Ceilings, walls and raised floors (to include platforms or stages) will be equipped with sufficient inspection ports to allow access to the entire cavity. In most locations, alarm systems should be installed to provide additional security in the space behind the false ceiling, wall and floor.

20. **Heating and Air Conditioning Ducts.** Must not allow physical, visual, or aural access to the TSA or information in it:

a. **Interior dimensions** that are 15 cm or larger, shall be protected with either steel bars, expanded metal grills, commercial metal sound baffles or an Intrusion Detection System.

b. **Solid steel bars** will be 1 cm in diameter (installed vertically and horizontally) on 15 cm centres, welded at all intersections.

c. **Expanded steel mesh** will be 9-gauge (or equivalent). Both solid steel bars

and expanded steel mesh will be solidly imbedded in the wall to a depth of no less than 15 cm.

21. **Security of ducts or vents** exiting the TSA will be enhanced by:

a. Being wrapped in sound absorbent material or equipped with non-conductive sections located within the TSA as near the perimeter wall as possible.

b. Having acoustical baffles installed in the ducts adjacent to the interior perimeter.

c. Having sufficient access ports to allow for effective visual inspections.

22. **Pipes.** In all new construction of TSAs, if feasible, pipes will be fitted with non-conducting tubing immediately adjacent to the interior perimeter to prevent the passing of structure borne audio. In existing structures and new structures where it is not feasible to use non-conducting sections, the pipes will be isolated from the classified sound sources. Protective measures that may be used include wrapping the pipes with sound deadening material and/or constructing a sound isolation barrier such as a false ceiling or wall between the pipes and the discussion area.

WIRING

23. All unused electrical and communications wires will be removed from within the TSA. If this is not feasible, the wires will be bound together and connected to earth ground or otherwise made unusable.

24. In newly designed TSAs, electrical wiring will exit the facility at a common single location. Wiring will be equipped with inspection panels (e.g. additional circuit breaker boxes) inside the TSA at the point the wiring breaches the perimeter.

25. All non-secure communications wiring will exit through the perimeter of the TSA at a single location. This exit point will be equipped with inspection panels inside the TSA at the point where it breaches the perimeter. All wires within the inspection panel will be specifically identified as to current use.

26. **Acoustical Isolation.** The perimeter (walls, doors, windows, etc.) of TSAs will be constructed so that room conversations and other audio originating within the facility cannot be recovered as intelligible audio outside the zone without the aid of electronic equipment.

27. **Apertures.** All apertures (cracks, holes, etc. but not doors or windows) which breach the perimeter of TSAs will be filled with a material equal to or greater than the strength of the original construction.

28. **Windows.** If windows are authorised, they will not be below 5.5 meters above uncontrolled ground, roofs, ledges, etc. They will be secured by heavy gauge wire of at least 3 mm in diameter, interwoven not more than 3 cm apart, and adequately secured to the exterior wall. Windows will be secured to prevent their being opened. They will have opaque coverings, blinds or drapes.

29. **Doors.** Doors in TSAs will be kept to a minimum. If more than one door exists, one

door will be used as the primary entrance and all other doors will be secured and used only in case of emergency.

a. **Perimeter Doors.** All perimeter doors in TSAs will be of solid wood, at least 4 cm thick and free of holes, cracks, abrasions; or they will be covered with steel sheeting that is at least 2 mm thick. The hinges will be located on the inside; or the hinge pins will be brazed, peened, pinned or welded to prevent unauthorised removal of the door. In no instance will glass doors or overhead door transoms be authorised for use as perimeter doors to TSAs.

b. **Entrance Doors.** Entrance doors will be fitted with built-in, NATO Group A changeable combination lock. A 4 mm solid hardened steel plate will be installed between the lock case and the interior of the door. If the aforementioned locking device cannot be immediately purchased and/or installed, the use of a highly pick resistant, mortise type 5 or 6 pin tumbler lock, equipped with at least a 25 mm solid steel dead bolt, is authorised on an interim basis, until the NATO Group A lock can be obtained. Should the mortise type 5 or 6 pin tumbler lock be used as an interim measure, the key and duplicates must be handled as security keys.

c. **Visitors, Maintenance and Cleaning Employees.** All visitors, maintenance crews and cleaning employees will be escorted at all times while in TSAs as governed by paragraphs of this Chapter.

30. **Intrusion Detection Systems.** Sensitive Zones that are not 24-hour manned will be protected by an Intrusion Detection System (IDS). Annex A provides details for IDS installation and maintenance.

31. **Non-Citable Findings.** Circumstances may arise where technical or physical security weaknesses are discovered but not covered by this directive or the ACO SOP on Technical Security. These circumstances may be due to technological advances or inadvertent exclusion of unforeseeable security problems; therefore, this paragraph is intended to allow flexibility to the Technical Security programme. Non-citable findings will be included in the exit briefings and investigative reports.

SECURITY STANDARDS DURING FIELD / COMBAT OPERATIONS

32. **Concept.** Security standards for field or combat operations can only prescribe the minimum requirements, since each situation differs. Situations and time permitting, the minimum standards below will be improved upon using the security considerations and requirements for permanent TSAs as an ultimate goal. If available, permanent type facilities will be used. Under field or combat conditions, continuous (24 hour) protection of the TSA is mandatory. Every effort must be made to obtain all necessary support from the headquarters served (e.g. security containers, vehicles, generators, fencing, automatic weapons, etc.).

33. **Minimum Requirements.** The following minimum physical security requirements will be met during field/combat operations.

a. The TSA will be physically located well within the supported headquarters defensive perimeter, preferably adjacent to the Operations Centre.

b. The TSA will be located within a controlled area surrounded by

concertina/barbed wire.

c. Walking or fixed guards will control the perimeter to provide observation of the entire controlled area. Guards will be armed with weapons and ammunition prescribed by the supported commander.

d. Access into the controlled area will be restricted to a single gate/entrance.

e. The gate/entrance to the controlled area will be guarded on a 24-hour basis.

f. A current access list will be maintained and access to the controlled area will be restricted to those personnel who have a "need-to-know" and possess the appropriate security clearance.

g. A minimum of two properly cleared personnel will be within the facility at all times.

h. Emergency destruction and evacuation plans will be kept current.

i. When not in use, material will be stored in approved security containers.

j. Communications, both wire and radio, if possible, will be established with and maintained with the reserve guard force.

34. **Temporary Relocation of Permanent Facilities.** TSAs facilities may be relocated to a field configuration as specified herein without formal certification of the temporary facility.

35. **TSAs in Bunker.** The hardened construction of bunkers with limited personnel access, controlled entry points, and roving guards/military police patrols greatly reduces the clandestine technical surveillance threat posed by Hostile Intelligence Services (HIS). Technical security for TSAs within bunkers should focus upon preventing the casual/inadvertent disclosure of sensitive information. It is not feasible to prescribe a complete list of physical/technical security criteria applicable to such facilities. Therefore, bunkers will be evaluated on a case-by-case basis. In addition to the minimum standards for TSAs, the following additional points should be considered.

a. **Ducts.** Usually associated with heating and air conditioning systems, ducts supply clean CBR-filtered air to the entire bunker complex. Disruption of this balanced airflow could negate the entire CBR overpressure system within the bunker. With this in mind, ducts must be designed and installed in such a manner as to limit and restrict physical, visual, and aural access to the TSA.

b. **Pipes.** Acoustical protective requirements for existing pipes will be recommended by the ACCI TSCM team and will be based on an evaluation of the actual threat posed by the pipes.

c. **Doors.** In bunkers with CBR overpressure systems, doors normally must be vented to the outside area. Doors that require vents will be equipped with a baffle system and cowl, which directs air flow to the floor.

ANNEX D TO
AD 070-001
DATED 22 DEC 21

TSA FACILITY PROFILE

1. **General.** This Annex outlines the documentation to be filed on each TSA in order to maintain a record of all action taken on a TSA.

2. **Responsibilities.** TSA Facility Managers are responsible for maintaining the TSA Facilities Profile in accordance with this Annex. ACCI elements are responsible for reviewing TSA Facilities Profiles for accuracy and completeness prior to conducting TSCM investigative services.

3. TSA Facilities Profiles will include all documentation of the TSA. At a minimum, the following information will be included:

a. Official designation by appropriate command authority of the TSA.

b. The most current TSA Certification.

c. A copy of the initial TSCM Investigative Survey.

d. A copy of the last TSCM Investigative Inspection Report.

e. Copies of any Waiver Certificates granted.

f. Plan and Place diagrams of the facility. Plan and Place diagrams will include floor plan drawings of the facility. These plans can be individual drawings or one drawing with overlays. Plan and Place diagrams will include the following:

(1) Electrical power runs and filters.

(2) Communications wire runs, filters, and telephone instrument placements.

(3) Pipes and ducts.

(4) IDS alarm system placements.

g. ADP equipment placement. Copies of all work orders or requests.

h. Access control procedures.

i. IDS alarm log (if applicable).

ANNEX E TO
AD 070-001
DATED 22 DEC 21

SECURITY ALERT STATES AND COUNTERMEASURES

INTRODUCTION

1. **NATO Security Alert States.** Security arrangements for the protection of NATO organisations (including official residences, clubs, messes, and domestic areas i.e. non-classified areas) are to be established in accordance with Appendix 1 to this Annex and promulgated through local orders. The security alert states ALPHA to DELTA reflect an increasing perceived threat and therefore increasing security measures. Wherever possible, commanders should aim to identify what threat(s) is present in order to assist in the selection of the most appropriate measures and/or the development of additional, location specific measures. It should be noted that where NATO organisations are located in a NATO HN, the HN may specify measures in addition to those in Appendix 1.

2. **Definitions.** The four security alert states are defined as follows:

a. **ALPHA.** Terrorist activity against NATO organisations and personnel is possible; however, there is no indication of a direct threat to NATO. NATO personnel and installations are to maintain a security posture sufficient to deter potential attacks.

b. **BRAVO.** There is an increased and more predictable threat of terrorist attack, which may target NATO installations and personnel. NATO personnel and installations are to implement an increased security posture in order to deter and counter potential attacks.

c. **CHARLIE.** An incident has *occurred* or intelligence has been received indicating that some form of terrorist action against NATO organisations and personnel is highly likely. NATO personnel and installations are to implement an increased security posture in order to defeat potential attacks.

d. **DELTA.** It is assessed that a terrorist action against a specific location or person is imminent or a terrorist attack has taken place. Normally, this alert state is issued as a localised warning and indicates the probability of an attack within the next 24-hour period. NATO installations are to implement an increased security posture in order to deny potential or further attacks.

DECLARATION OF ALERT STATES AND IMPLEMENTATION OF MEASURES

3. The declaration of Alert States may be decreed by the HN, by a superior formation as a result of intelligence received, or by the local commander following receipt of intelligence through official sources, following an anonymous threat message or as the result of a local incident.

4. The baseline, minimum Alert State is set and declared ACO-wide by SACEUR. Thereafter, Alert States are decreed by the superior formation and may be influenced by the HN; in extremis, the Alert State may be locally declared by the relevant NATO Commander following receipt of intelligence through official sources, following an anonymous threat message or as the result of a local incident.

5. A selection of measures are mandatory, however, the diversity and geographic expanse of the Alliance is such that the recommended measures will need to be tailored for local conditions and local measures will need to be developed. The Alert State declared by a NATO Commander is mandatory for all the NATO personnel and installations in its Command Area of Responsibility. In case it is considered necessary, the Alert State could be increased in some specific location. Should a local NATO Commander raise the formation / installation Alert State, the ascending chain of command must be advised immediately. The measures at Appendix 1 do not represent all possible countermeasures and commanders may introduce additional measures as they deem necessary. Alert States may be confined to the geographical area deemed at risk. Following the guidance in Appendix 1, the mandatory measures in each Alert State are to be implemented and the discretionary ones depending on each Commander's decision. NATO Commanders retain the prerogative to implement measures in addition to those aligned with the relevant Alert State in Appendix 1 – an indication of this will be given by the addition of "PLUS" as a descriptor to the Alert State. All unofficial information received should always be referred to the HN security authorities for authentication in parallel with any precautionary security measures.

6. **Intelligence and Higher Commanders Intent.** Wherever possible, should superior formations deem it necessary to increase the Alert State, an explanation of the underlying reasoning for the increase should be included in the Alert State Message. The Alert State and accompanying countermeasures should be designed to counter the specific threat(s) identified. To assist in this process, when issuing an Alert State Message, a superior formation should include '*Higher Commanders Intent*' (or '*Desired End-State*') in the message to help shape the thinking of subordinate units.

7. **Weapons and Ammunition.** Local orders are to include specific instructions concerning the issue of weapons and live ammunition to guards and to sentries. Any such orders must comply with the policy/laws of the HN and of the NATO organisation concerned.

8. **Implementation at Integrated Units.** The detailed measures to be adopted by NATO organisations where they share facilities with national formations will need to be co-coordinated with the latter. In the case of NATO formations located within national installations which are already subject to well established national counterterrorist systems/procedures for their protection, there is no requirement to replace that system with the one outlined in this Chapter.

9. **Classification of Alert States.** The full definitions of the alert states are NATO UNCLASSIFIED. Declarations of alert states should normally be NATO UNCLASSIFIED but explanatory or amplifying messages must be classified according to content.

APPENDIX:

1. NATO Alert States and Measures Table.

APPENDIX 1 TO
ANNEX E TO
AD 070-001
DATED 22 DEC 21

NATO ALERT STATES AND MEASURES TABLE

NATO ALERT STATE				
	ALPHA	**BRAVO**	**CHARLIE**	**DELTA**
Definition	Terrorist activity against NATO organisations and personnel is possible; however, there is no indication of a direct threat to NATO. NATO personnel and installations are to maintain a security posture sufficient to deter potential attacks.	There is an increased and more predictable threat of terrorist attack, which may target NATO installations and personnel. NATO personnel and installations are to implement an increased security posture in order to deter and counter potential attacks.	An incident has occurred or intelligence has been received indicating that some form of terrorist action against NATO organisations and personnel is highly likely. NATO personnel and installations are to implement an increased security posture in order to defeat potential attacks.	It is assessed that a terrorist action against a specific location or person is imminent or a terrorist attack has taken place. Normally this alert state is issued as a localised warning and indicates the probability of an attack within the next 24-hour period. NATO personnel and installations are to implement an increased security posture in order to deny potential or further attacks.
Measures				
Preparedness	**Measure A1 (Mandatory).** Review all plans, orders, personnel details and logistics requirements related to the introduction of higher Alert States. Plans should ensure that sufficient duty staffs are either at work or on-call to respond to incidents and implement higher Alert States.	**Measure B1 (Mandatory).** Review all plans, orders, personnel details and logistics requirements related to the introduction of higher Alert States. Plans should ensure that sufficient duty staff are either at work or on-call to respond to incidents and implement higher Alert States.	**Measure C1 (Mandatory).** Review all plans, orders, personnel details and logistics requirements related to the introduction of higher Alert States. Plans should ensure that sufficient duty staff are either at work or on-call to respond to incidents and implement higher Alert States.	**Measure D1 (Not Used).**
	Measure A2 (Discretionary). Move possible IED containers such as vehicles and dustbins etc. as far as practicable from occupied buildings.	**Measure B2 (Discretionary).** Move possible IED containers such as vehicles and dustbins etc. as far as practicable from occupied buildings.	**Measure C2 (Discretionary).** Move possible IED containers such as vehicles and dustbins etc. as far as practicable from occupied buildings.	**Measure D2 (Discretionary).** Move possible IED containers such as vehicles and dustbins etc. as far as practicable from occupied buildings.
	Measure A3 (Not Used).	**Measure B3 (Discretionary).** Take preparatory measures to reduce vulnerability to VBIEDs, such as installing ramps / chicanes and blast protection.	**Measure C3 (Discretionary).** Take preparatory measures to reduce vulnerability to VBIEDs, such as installing ramps/ chicanes and blast protection.	**Measure D3 (Mandatory).** Take preparatory measures to reduce vulnerability to VBIEDs, such as installing ramps/ chicanes and blast protection.
	Measure A4 (Not Used).	**Measure B4 (Discretionary).** Consult local authorities regarding security measures for higher alert states including closing public roads and monitoring potential locations for launch of stand-off weapons, indirect fire or sniper fire.	**Measure C4 (Discretionary).** Consult local authorities regarding security measures for higher alert states including closing public roads and monitoring potential locations for launch of stand-off weapons, indirect fire or sniper fire.	**Measure D4 (Mandatory).** Consult local authorities regarding security measures for higher alert states including closing public roads and monitoring potential locations for launch of stand-off weapons, indirect fire or sniper fire.

Measures	ALPHA	BRAVO	CHARLIE	DELTA
Awareness	**Measure A5 (Mandatory).** All personnel, including dependents, are to be reminded at least annually of the need to remain vigilant and to be inquisitive about strangers and any other unusual activity. Briefings should aim to maintain confidence, stop rumours and prevent alarm.	**Measure B5 (Mandatory).** All personnel, including dependents, are to be reminded at least quarterly of the need to remain vigilant and to be suspicious and inquisitive about strangers; be alert for unidentified vehicles , abandoned parcels or suitcases or any other unusual activity on, or in the vicinity of NATO organisations. Briefings should aim to maintain confidence, stop rumours and prevent alarm.	**Measure C5 (Mandatory).** All personnel, including dependents, are to be reminded at least weekly of the need to remain vigilant and to be suspicious and inquisitive about strangers; be alert for unidentified vehicles on, or in the vicinity of NATO organisations; abandoned parcels or suitcases or any other unusual activity. Briefings should aim to maintain confidence, stop rumours and prevent alarm.	**Measure D5 (Mandatory).** All personnel, including dependents, are to be updated on the current security measures adopted; be alert for unidentified vehicles on, or in the vicinity of NATO organisations; abandoned parcels or suitcases or any other unusual activity. Briefings should aim to maintain confidence, stop rumours and prevent alarm.
Visibility	**Measure A6 (Not Used).**	**Measure B6 (Discretionary).** Restrict the wearing of uniform off-base.	**Measure C6 (Mandatory).** Restrict the wearing of uniform off-base.	**Measure D6 (Mandatory).** Prevent the wearing of uniform off-base.
	Measure A7 (Mandatory). Advise staff and dependents how to lower their visibility at home and online.	**Measure B7 (Mandatory).** Advise staff and dependents how to lower their visibility at home and online.	**Measure C7 (Mandatory).** Advise staff and dependents how to lower their visibility at home and online.	**Measure D7 (Mandatory).** Advise staff and dependents how to lower their visibility at home and online.
	Measure A8 (Discretionary). Advise staff on measures to protect NATO transport when off- base.	**Measure B8 (Discretionary).** Direct staff to take measures to protect NATO transport when off-base.	**Measure C8 (Mandatory).** Direct staff to take measures to protect NATO transport when off- base.	**Measure D8 (Mandatory).** Direct staff to take measures to protect NATO transport when off- base.
	Measure A9 (Not Used).	**Measure B9 (Not Used).**	**Measure C9 (Discretionary).** Limit all inbound and outgoing administrative journeys and visits.	**Measure D9 (Mandatory).** Limit all inbound and outgoing administrative journeys and visits.
	Measure A10 (Not Used).	**Measure B10 (Not Used).**	**Measure C10 (Discretionary).** Cease all non- essential tasks and activity.	**Measure D10 (Mandatory).** Cease all non-essential tasks and activity.
	Measure A11 (Not Used).	**Measure B11 (Discretionary).** Vary staff working hours in order to minimise congestion at entry points.	**Measure C11 (Mandatory).** Vary staff working hours in order to minimise congestion at entry points.	**Measure D11 (Mandatory).** Vary staff working hours in order to minimise congestion at entry points.
Control of Entry	**Measure A12 (Mandatory).** All visitors to NATO installations are to be occasionally subject to an identity check prior to entry and their vehicles subject to search on entry, if authorised and required.	**Measure B12 (Mandatory).** All visitors to NATO installations are to be regularly subject to an identity check prior to entry and their vehicles subject to search on entry, if authorised and required.	**Measure C12 (Mandatory).** All visitors to NATO installations and members of staff are to be frequently subject to an identity check prior to entry and their vehicles subject to search on entry, if authorised and required.	**Measure D12 (Mandatory).** All visitors to NATO installations are to be subject to an identity check prior to entry and their vehicles subject to search on entry, if authorised and required.
	Measure A13 (Mandatory). All permanent staff of NATO installations are to be occasionally subject to an identity check prior to entry, which may be undertaken by an automated system.	**Measure B13 (Mandatory).** All permanent staff of NATO installations are to be regularly subject to an identity check prior to entry, which may be undertaken by an automated system.	**Measure C13 (Mandatory).** All permanent staff of NATO installations are to be frequently subject to an identity check prior to entry: automated systems may only be used if both identification and authentication processes are active. Security and Non-security cleared personnel entering security areas within NATO installations are to be frequently subject to search on entry.	**Measure D13 (Mandatory).** All permanent staff of NATO installations is to be continuous subject to an identity check prior to entry: automated systems may only be used if both identification and authentication processes are active. Security and Non-security cleared personnel entering security areas within NATO installations are to be occasionally subject to search on entry.

Measures	ALPHA	BRAVO	CHARLIE	DELTA
	Measure A14 (Not Used).	**Measure B14 (Mandatory).** Ensure effective security at each Control of Entry location: if necessary, limit access points to concentrate security resources; however, excessive queues should be avoided.	**Measure C14 (Mandatory).** Ensure robust security at each Control of Entry location: if necessary, limit access points to concentrate security resources; however, excessive queues should be avoided.	**Measure D14 (Mandatory).** Ensure highly robust security at each Control of Entry location: if necessary, limit access points to concentrate security resources; however, excessive queues should be avoided.
	Measure A15 (Not Used).	**Measure B15 (Discretionary).** Dispose physical devices with the purpose of slowing down or even stopping incoming vehicles approaching entry point, such as ramps and chicanes.	**Measure C15 (Discretionary).** Erect ramps and chicanes to reduce vehicle speed on approach to entry points.	**Measure D15 (Discretionary).** Erect ramps and chicanes to reduce vehicle speed on approach to entry points.
Search	**Measure A16 (Discretionary).** Non-security cleared personnel visiting NATO installations and their vehicles are to be occasionally subject to search on entry when entering the installation and/or security areas within it.	**Measure B16 (Discretionary).** Non-security cleared personnel visiting NATO installations and their vehicles are to be regularly subject to search on entry when entering the installation and/or security areas within it.	**Measure C16 (Mandatory).** Non-security cleared personnel visiting NATO installations and their vehicles are to be frequently subject to search on entry when entering the installation and/or security areas within it.	**Measure D16 (Mandatory).** All Non-security cleared personnel visiting NATO installations and their vehicles are to be subject to search on entry when entering the installation and/or security areas within it.
	Measure A17 (Discretionary). Security cleared personnel entering NATO installations and their vehicles are to be occasionally subject to search on entry when entering the installation and/or security areas within it.	**Measure B17 (Discretionary).** Security cleared personnel entering NATO installations and their vehicles are to be occasionally subject to search on entry when entering the installation and/or security areas within it.	**Measure C17 (Mandatory).** Security cleared personnel entering NATO installations and their vehicles are to be occasionally subject to search on entry when entering the installation and/or security areas within it.	**Measure D17 (Mandatory).** Security cleared personnel entering NATO installations and their vehicles are to be occasionally subject to search on entry when entering the installation and/or security areas within it.
	Measure A18 (Discretionary). Mail is to be occasionally examined for suspicious articles.	**Measure B18 (Discretionary).** Mail is to be regularly examined for suspicious articles.	**Measure C18 (Discretionary).** All mail is to be examined for suspicious articles.	**Measure D18 (Discretionary).** All mail is to be prevented from entering NATO installations.
Patrolling & Surveillance	**Measure A19 (Mandatory).** Conduct occasional, visible patrols to maintain surveillance, deter attackers and provide confidence to staff and dependents.	**Measure B19 (Mandatory).** Conduct regular, visible patrols to maintain surveillance, deter attackers and provide confidence to staff and dependents.	**Measure C19 (Mandatory).** Conduct frequent, visible patrols to maintain surveillance, deter attackers and provide confidence to staff and dependents.	**Measure D19 (Mandatory).** Conduct continuous, visible patrols to maintain surveillance, deter attackers and provide confidence to staff and dependents.
	Measure A20 (Discretionary). Ensure that patrols of external installations perimeter, domestic accommodation, schools, messes, social facilities and other soft targets off-base are conducted: any such activity must be coordinated with relevant HN agencies.	**Measure B20 (Mandatory).** Ensure that occasional patrols of external installations perimeter, domestic accommodation, schools, messes, social facilities and other soft targets off-base are conducted: any such activity must be coordinated with relevant HN agencies.	**Measure C20 (Mandatory).** Ensure that regular patrols of external installations perimeter, domestic accommodation, schools, messes, social facilities and other soft targets off-base are conducted: any such activity must be coordinated with relevant HN agencies.	**Measure D20 (Mandatory).** Ensure that continuous patrols of external installations perimeter, domestic accommodation, schools, messes, social facilities and other soft targets off-base are conducted: any such activity must be coordinated with relevant HN agencies.
	Measure A21 (Discretionary). Buildings, rooms and cupboards not in regular use should be secured.	**Measure B21 (Mandatory).** Buildings, rooms and cupboards not in regular use should be secured.	**Measure C21 (Mandatory).** Buildings, rooms and cupboards not in regular use should be secured and inspected regularly.	**Measure D21 (Mandatory).** Buildings, rooms and cupboards not in regular use should be secured and inspected regularly.
	Measure A22 (Discretionary). Improve surveillance by maintaining a clear area around buildings.	**Measure B22 (Discretionary).** Improve surveillance by maintaining a clear area around buildings.	**Measure C22 (Mandatory).** Improve surveillance by maintaining a clear area around buildings.	**Measure D22 (Mandatory).** Improve surveillance by maintaining a clear area around buildings.

Measures	ALPHA	BRAVO	CHARLIE	DELTA
	Measure A23 (Discretionary). Occasionally inspect areas outside buildings for suspicious articles or evidence of intruders.	**Measure B23 (Discretionary).** Regularly inspect areas outside buildings for suspicious articles or evidence of intruders.	**Measure C23 (Mandatory).** Frequently inspect areas outside buildings for suspicious articles or evidence of intruders.	**Measure D23 (Mandatory).** Continuously inspect areas outside buildings for suspicious articles or evidence of intruders.
	Measure A24 (Not Used).	**Measure B24 (Discretionary).** Maintain surveillance of critical infrastructure.	**Measure C24 (Discretionary).** Protect critical infrastructure.	**Measure D24 (Discretionary).** Protect critical infrastructure.
Response	**Measure A25 (Discretionary).** An armed response force is to be available to react to security incidents.	**Measure B25 (Discretionary).** An armed response force is to be available to react to potential security incidents.	**Measure C25 (Mandatory).** An armed response force, of sufficient size to defeat expected attacks, is to be available to counter security incidents.	**Measure D25 (Mandatory).** An armed response force, of sufficient size to defeat expected attacks, is to be available to counter security incidents.
	Measure A26 (Mandatory). Protective equipment for security personnel is to be available at their place of work.	**Measure B26 (Mandatory).** Protective equipment for security personnel is to be immediately available	**Measure C26 (Mandatory).** All security personnel are to wear protective equipment when on post and are to remain immediately available at all other times.	**Measure D26 (Mandatory).** All security personnel are to wear protective equipment when on post and are to remain immediately available at all other times.

ANNEX F TO
AD 070-001
DATED 22 DEC 21

PLANNING NOTES FOR PROTECTION AGAINST ATTACK

INTRODUCTION

1. This Annex is designed as an aide memoire to assist locations in preparing their own plans to protect against attack and should be read in conjunction with extant Host Nation (HN) regulations. It is provided for guidance and should only be used as a planning tool; local procedures must be developed to suit local conditions. The contents of this Annex should not be considered as a complete guide and appropriate Subject Matter Experts (SMEs) (both NATO and HN) must be involved in producing local Direction and Guidance (D&G). The local Chain of Command must be fully engaged in planning and all personnel should be briefed and, if necessary, exercised in any plan(s).

PRIMACY AND RESPONSIBILITY

2. This Annex has been written primarily for use at established NATO Installations ('the home-base') in peacetime. It is considered that both primacy and the majority of any response will rest with the HN. Nevertheless the Countermeasures detailed at Annex E must also be used as a basis for planning in any theatre of operations.

PRINCIPLES OF INCIDENT MANAGEMENT

3. Incident Planning must take into account the five main principles of Incident Management (Confirm, Clear, Cordon, Control & Communicate – often referred to as the 5Cs):

a. **Confirm.** Personnel should be encouraged to report anything suspicious without fear of sanction if initial suspicions are found to be incorrect. Until any incident is declared as a false alarm, all personnel should behave as an incident presents a real threat to life and property. Consideration should be given to providing to all staff a simple reporting form for outlining the information that will be required by the emergency services and any Incident Management Team. This principle sounds the easiest to establish, however, in reality confirming some incidents can be difficult. For example, is a suspicious package or an apparently abandoned bag an Improvised Explosive Device (IED)? If in doubt, an incident should be declared and all necessary measures taken until an appropriately qualified specialist both confirms and directs further action or, declares a false alarm/hoax. As part of daily routine, a check of local environs / buildings / offices before occupancy is called 'Op WIDEAWAKE' – this can be extended following the declaration of an Incident to compel personnel to remain indoors; restrict movement around the Installation to a minimum; office occupants are to identify all personnel within their office and check their immediate areas for suspicious devices / packages. Any suspicious activity / packages must be reported immediately to the local security coordinator.

b. **Clear.** The purpose of clearing an area is to move people away from any risk to a place of safety. This may be achieved by a partial evacuation on large installations and the incident area is small or, a full evacuation in the event of a large incident (or small installation). The clearing of an incident area must be

conducted quickly, efficiently and above all calmly. It is often the case that many injuries are suffered during the clearing of an incident area, rather than as a result of the incident itself. It must be ensured, particularly when dealing with large numbers of civilians, that panic does not prevail. It is important that personnel evacuating any area are provided with the following information (to ensure that they do not place themselves in further danger):

(1) The nature/type of incident that is occurring.

(2) The actual location of the incident.

(3) The location of the evacuation point.

(4) The route to be used to get to the evacuation point.

Note: The evacuation point and the route to it must be cleared before being used to ensure both are safe for use by large numbers of people. It should be remembered that for evacuations to be done well, they must be thoroughly practised. Movement away from the suspected device should use available cover and remain out of 'line of sight' of the suspected device.

c. **Cordon.** A cordon should be established in order to prevent people from entering the area of the incident, thus endangering their lives. It will also help to preserve the scene of the incident, enabling security agencies to conduct their investigations. When establishing a cordon, several points could be considered, which can be seen at Appendix 1 to this Annex.

d. **Control.** Command and Control (C2) of the incident must be established as soon as possible. The C2 of any incident will remain with installation personnel until specialist/HN agencies can take over. The control of an incident could be managed by using Forward Control Points (FCP), Incident Control Points (ICP), Emergency Services Rendezvous Points (ERV) and Evacuation Assembly Points (EAP) as described in Appendix 1.

e. **Communicate[20].** It is vital that there is a free flow of communication both up and down the incident management chain. The FCP must recognise the objectives of the ICP and thus should keep it fully informed. In the same manner, the ICP must recognise that the FCP is dealing with the tactical issues of the incident and will not have the capacity to provide countless situation reports. The flow of information is a balancing act which can only be achieved by practice. Too much information flow can be just as detrimental as too little.

4. **Three Examples of Incidents.** Three example scenarios of possible incidents are given below; these are relevant to all Incident Planning but actual responses must be coordinated with the HN:

a. **Demonstration and Riots.** It is unlikely that NATO personnel will be involved in dealing with demonstrations or riots in peacetime. Indeed, some nations have national caveats that prevent military personnel from engaging in such activity

[20] 'Communicate' may be replaced as the 5th 'C' with 'Call'.

at any time. Continuing to operate, protecting vital facilities, protecting personnel and maintaining the positive reputation of the Alliance should be key planning considerations. Further, successfully protecting against the effects of demonstrations and riots can only be achieved through pre-planning and coordination between all those involved in providing such protection. The primary responsibility for responding to demonstrations and riots rests with the government of the HN. However, responsibility for the internal protection of installations and personnel lies with Commanding Officers and Heads of Agencies. Appendix 2 lists some options for consideration when planning local responses.

b. **Explosive Devices / Postal Bombings.** It is possible that NATO personnel may face the threat from explosive devices or postal bombings; therefore, preventive steps should be taken and countermeasures planned for such an attack. The threat emanates from a number of vectors such as use of stolen military ordnance to the construction of crude incendiary devices or more complex improvised explosive devices. In the context of this document, the term Improvised Explosive Device (IED) will be used for the range of threat vectors. Appendix 2 provides guidance to assist in reviewing existing plans or in formulating new plans to deal with the threat from IEDs and the events following an IED detonation. Issues suggested for consideration are listed under the following headings: Preventive Steps, 'Bomb Threats', IED Discovery and IED Detonation / Recovery. The postal (mail) bomb threat consists of two categories that are differentiated by size: letter-IEDs (including 'book-bombs') and the standard package / parcel IED.

c. **Terrorist Attack.** There is a potential risk that terrorist organisations may target a NATO installation to kidnap a particular individual, to take hostages, or to occupy or damage important installations. Terrorists choose targets for their potential publicity value and weak defences, rather than solely for an ideological reason. The majority of NATO installations are sufficiently well protected to discourage all but the most well planned or determined attack. However, the rise of extremism and the desire of some attackers to be martyred have profound consequences for security and the issue of the suicide attacker must be carefully considered by security professionals. A successful attack will almost always take place without adequate warning. The defences of the target will have been carefully reconnoitred beforehand. Without large expenditure and placing excessive restrictions on the daily life of an installation, it is not possible to guarantee that any Installation Security Plan (ISP) could prevent or detect a penetration. The ISP should therefore provide for the contingency of the terrorists' presence first becoming known after the outer defences have been penetrated. Such provisions should include immediate measures to prevent terrorists from escaping with or without a kidnap or hostage victim or progressing further into an installation. A well-conceived plan, coordinated with HN security agencies, which is well exercised and understood, coupled with clear command responsibilities and good communications, offers the best chances of effectively dealing with an attack. This combination will almost certainly become apparent to terrorists during their reconnaissance and will have the best chance of discouraging them from mounting an attack. Additional points to be considered can be found in Appendix 2.

5. **Protection Measures to be Taken outside NATO Facilities.** The collective protection offered by NATO installations cannot be extended outside the premises and terrorists may thus choose the easier option of attacking personnel (or their families, to

include civilian workers and contractors) in the vicinity of, but away from, a NATO location. Homes, especially those isolated from other NATO personnel, are most at risk in this respect and risk may increase with the rank of the occupant. The role/function of the NATO facility will be a factor in considering threat and the threat may increase due to the country of origin of an individual. Personnel may also be at risk when travelling to and from their place of duty. All NATO personnel should consider themselves potential terrorist targets and should take reasonable and proportionate self-protection measures, according to their personal situation. For example, travel to and from work whilst in uniform should be avoided at all times, but advice and guidance can always be accessed through the Chain of Command. Planning considerations for Protection Measures outside NATO facilities are provided at Appendix 3.

6. Overall, the most effective protective measures are those that convince the terrorist during their surveillance, that the potential victim is too elusive, too alert or too well protected for an attack to have a sufficiently good chance of success. Protection of personnel on NATO installation will be provided for by the Chain of Command and by the HN off-base. These two areas whilst distinct cannot be treated in isolation and protective measures must be seamless. Close liaison between the Chain of Command and the HN is vital and should be considered as routine essential activity. The best protection will be afforded by a series of well-considered and coordinated protective measures that exist in depth and with realistic alternatives considered in case of a major incident. Appropriate SMEs should be prepared, after liaison with the necessary HN authorities, to provide advice and guidance on protective measures and assist in their implementation.

APPENDICES:

1. Principles of Incident Management.
2. Exemplar Planning Considerations – Three Types of Incident.
3. Protection Measures outside NATO Facilities.

APPENDIX 1 TO
ANNEX F TO
AD 070-001
DATED 22 DEC 21

PRINCIPLES OF INCIDENT MANAGEMENT

1. **Cordon.** The following points could be considered when establishing a cordon:

   a. **Danger Area.** Any cordon must be established beyond the area of danger; it should not be within line of sight of an explosive device. The distance of the cordon from the scene of the incident will be defined by the size of the threat or suspect device; the larger the device, the bigger the cordon. The presence of 'hard cover' between any threat and personnel may allow the size of the cordon to be reduced. Recommended Safety Distances are[21]:

      (1) Briefcase-sized device = 100m.

      (2) Vehicle-Borne Threat / 'Car Bomb' = 200m.

      (3) Large Improvised Explosive Device (IED) = 400m (includes van and truck bombs, or where secondary hazards are present e.g. Fuel Storage facilities).

      (4) The Chain of Command may change these guidelines based on the prevailing situation.

   b. **Checks.** Each cordon position must be checked before occupation for further danger. This could include flammable substances, insecure structures, smoke or possible secondary devices in the event of a bomb threat. Checks are achieved by conducting a 5 m search around the area in which the cordon is to be established. If the cordon position is to be established for a protracted period of time, the search should be extended to 20 m.

   c. **Cordon Control.** The manning of the cordon position requires firm control. In the event of an incident the natural reaction of personnel is to be inquisitive or to go forward to offer help; to be effective a cordon must be kept secure.

   d. **Single Point of Entry.** Any cordon should only have one exit and entry point. All specialist personnel should use this point and a route should be established from the cordon entry point to the site of the incident. This route should again be checked to ensure it is safe prior to use.

2. **Control.** The control of an incident could be managed as follows:

   a. **Forward Control Point (FCP).** The FCP will be located on the cordon line and will be the only entry and exit point to the incident. Once the FCP has been established it should inform the ICP immediately. The function of the FCP is to tactically manage the incident and to control the cordon. Details of persons manning the cordon should be passed to the ICP, so that they can produce a list of personnel accounted for. It should remain in position until relieved by specialists or

[21] NATO Standard AEODP-03, Volume II, Para 1.7. Safety Distances.

HN emergency services.

b. **Incident Control Point (ICP).** The ICP will be located well away from the scene of the incident. It is from this point that the incident will be controlled.

c. **Emergency Services Rendezvous Point (ERV).** On large installations an ERV should be pre-identified. The ERV is the point at which all emergency services will locate. It should be clearly marked and provide adequate access for emergency vehicles. The ERV should have communications with the ICP and when manned should inform the ICP that it is ready to receive the emergency services.

d. **Evacuation Assembly Point (EAP).** The EAP is the area to which all evacuated personnel should muster. This area should also be cleared prior to occupation to ensure there are no further hazards. Personnel should then be organised into medical and search teams as appropriate. It should be noted that larger installations will require a number of EAPs. It is possible that HN security agencies will require personnel to check their own work areas for anything suspicious[22].

[22] Op WIDEAWAKE is referenced in Annex F Para 3.a. – this also can be extended following the declaration of an Incident to compel personnel to remain indoors; restrict movement around the Installation to a minimum; office occupants are to identify all personnel within their office and check their immediate areas for suspicious devices / packages. Any suspicious activity / packages must be reported immediately to the local security coordinator.

APPENDIX 2 TO
ANNEX F TO
AD 070-001
DATED 22 DEC 21

EXEMPLAR PLANNING CONSIDERATIONS – THREE TYPES OF INCIDENTS

1. **Demonstration and Riots.** The following list are some options for consideration when planning local responses (this list should not be considered as either complete or prescriptive; it is provided for guidance only):

a. **Preparation Phase** (demonstration or riot considered likely):

(1) Ensure liaison with the appropriate security authorities of the HN is in place and ongoing.

(2) Review duty rosters and consider the assignment of additional duties if required by any developing situation.

(3) In consultation with the HN and higher headquarters when necessary, guarding of sensitive areas should be reviewed, to include storage of small arms ammunition, explosives, chemical riot control agents, etc. Consider facilities off- site which if targeted may have an impact on site (e.g. power, water, waste treatment and telecommunications facilities etc.).

(4) Consider evacuation of personnel and visitors from any location that could be at risk.

(5) Review access control measures. Consider that delaying access through increased security checks may create a queue of vehicles/personnel at Entry Control Points (ECPs) that could present a target for demonstrators.

(6) If feasible, consider establishing observation points with communications to warn of any threat. Ensure that warnings can be passed to the appropriate authorities in a timely manner to facilitate an appropriate and timely response.

(7) Consider the need to effectively communicate information and warnings effectively both internally and externally.

(8) Remove vehicles from any anticipated area of risk.

(9) In case of any emergency, can access and egress for emergency vehicles be maintained and controlled?

(10) Are any personnel at particular risk and require the provision of protective equipment?

(11) Review arrangements for emergency protection, evacuation or destruction of classified or locally sensitive material.

(12) Consider obtaining stocks of emergency rations and water to sustain staff that may be unable to leave the premises.

(13) In event of an incident, are emergency medical treatment and subsequent evacuation plans sufficiently robust for the developing situation?

(14) Local commanders should consider extant Rules of Engagement (ROE).

b. **Action Phase** (Demonstration or riot considered imminent):

(1) Understand and distribute as necessary the advice and recommendations of the HN security authorities.

(2) If necessary reinforce guarding of sensitive areas, including storage of small arms ammunition, explosives, chemical riot control agents, etc. Consider facilities off site, which, if targeted, may have an impact on-site (e.g. power, water, waste treatment and telecommunications facilities).

(3) Ensure ability to continue to communicate internally and externally in the event of an incident. Pay particular attention to ability to communicate with security and emergency services (fire, medical etc.).

(4) Close and lock gates, protective screens and doors. However, ensure that emergency evacuation routes can still be achieved.

(5) Close any windows and curtains/drapes/blinds facing the external perimeter of the installation and warn personnel to stay away from windows.

(6) Consider relocation of essential personnel into most secure areas of the facility. Any areas vacated should be secured.

(7) Relocate removable classified and/or valuable material into most appropriate secure storage locations.

(8) Be prepared for destruction of most sensitive classified information in accordance with emergency destruction plan.

(9) Consider threat of fire from explosive or incendiary devices and ensure most robust measures are in place to counter this threat. Consider a priority order for fire-fighting.

(10) Evacuate all non-essential personnel and visitors. Have a robust plan for the evacuation of all personnel.

(11) Clear any potential scene of confrontation of any objects that could be used as missiles[23] or weapons. Remove any combustible material or, if removal is not possible, consider soaking with water (if practicable) to minimise risk of fire.

2. **Explosive Devices / Postal Bombings.** Issues suggested for consideration as part of response planning are listed below:

[23] The term ‘missiles’ includes bricks, branches and other detritus that could be thrown at or used against NATO Friendly Forces.

a. **Preventive Steps**

(1) Education and Training on what is required in times of increased threat should take place on a regular basis. Each location's Induction Package should include actions required of all personnel in the event of an incident. In times of increased threat, additional training or further refresher training should be considered.

(2) During security training, personnel should be trained that when evacuating they should evacuate carrying whenever possible all first aid fire-fighting equipment and any incident response packs to include first aid packs and stretchers in order to ensure that such equipment is immediately available, should the situation deteriorate.

(3) A number of Incident Commanders should be identified and trained to ensure redundancy.

(4) Establish early liaison with HN specialists/experts who are likely to respond in the event of an incident. Liaison should be routine activity and not commence when a threat emerges or the Alert State changes. Building strong relationships will have enormous benefits if an incident does occur and rapid, robust action is required in times of immense personal stress (i.e. after an explosion). Consider running regular incident response exercises. Key members of the NATO Security/Force Protection/Incident Management Team should know their HN counterparts.

(5) Identify and train incident commanders and incident management teams and ICPs across the installation. Always have alternate solutions and redundancy built in. Ensure any ICP location is correctly cleared before occupation.

(6) Ensure that fire prevention plans are up-to-date, first aid fire-fighting equipment is serviceable. All emergency exits should be clear and useable. Evacuation plans should be regularly exercised and an Emergency Rendezvous point (ERV) identified. Alternative Rendezvous Points (RVPs) need to be identified and all personnel need to check any RVP prior to occupation to ensure no Secondary or indeed Tertiary Devices have been emplaced.

(7) Review access control measures. Consider that delaying access through increased security checks may create a queue of vehicles/personnel at ECPs that could present an opportunity target.

(8) Instruct any guards patrolling installations to be on the look-out for suspicious items left unattended, particularly in areas of mass-gathering (dining facilities, gymnasiums, cinemas etc.). Security staff must be properly trained in the actions required following the discovery of a suspicious item. In times of increased threat expect false alarms; do not discourage personnel from acting upon their suspicions for fear of criticism. Personnel should be encouraged to enter a daily routine of checks of facilities and accommodation before occupancy to check for anything suspicious.

(9) Advise security personnel to be alert for suspicious activity including suspicious personnel and vehicles (including unexpected or unusual deliveries) in the vicinity of the installation. Wherever possible note the persons' details and description and/or vehicle details (make, model, colour, registration/license plate number, any signage, details of occupants etc.) Consideration should be given to producing 'sighting sheets' to aid the capturing of data. Photographs and Closed Circuit Television (CCTV) images should be captured and stored if possible. Circulate details to HN security agencies and, if applicable, other NATO/national military facilities (consider person/vehicle may have been seen in vicinity of other locations).

(10) Ensure that vulnerable/sensitive areas have adequately physical protection.

(11) Ensure that doors to public areas, air-conditioner rooms, telephone panel rooms, lift/elevator machine rooms, cleaners cupboards/utility closets, etc. are locked when not in use.

(12) Inventory/test/check all security and emergency equipment on a regular basis (fire extinguishers, medical packs, security lighting, public address systems, emergency power supplies, alarms, sirens, etc.).

(13) Consider creating emergency first aid equipment pack-ups for dispersal across the facility.

(14) Ensure that all visitors are properly escorted and if the threat necessitates, are briefed on emergency procedures in the event of an incident.

b. **'Bomb Threats'.** If a threatening message is received:

(1) **By Telephone.** Record the call in detail. Note any background noises and as much detail as possible concerning the voice and manner of the caller. Keep the caller engaged for a long as possible on any pretext. If the recording of call is not possible, the recipient should be de-briefed in detail. During security education, personnel should be briefed on the handling of suspicious phone calls and consideration should be given to providing forms to be placed next to telephones to aid in capturing data.

(2) **Through the Mail.** Protect the mail from unnecessary handling to preserve evidence for subsequent scientific examination by the police or security authorities. If the threat warrants, basic forensic awareness training for personnel handling mail on a regular basis should be considered.

(3) The local Chain of Command should be alerted at the earliest opportunity. All threats should be reported to the HN security authorities and to the NATO Chain of Command.

(4) In consultation with HN security agencies, consider alerting other emergency response providers on an off-base (Explosive Ordnance Disposal teams, police, fire, medical etc.).

(5) If appropriate, alert all staff. Include support and maintenance staff (plumbers, electricians, etc.) as these personnel will often work in infrequently visited areas of the installation where a device could have been planted unseen.

(6) Decide whether to evacuate area completely, to evacuate on a limited scale, or not to evacuate at all. Establish appropriate crowd control where necessary. If evacuation is necessary, ensure that the evacuation assembly points are cleared and safe before occupation. In all cases ensure an adequate flow of information to all staff.

(7) Ensure a method of accounting for all staff is in place. If any doubt exists, personnel not accounted for should be reported as such at the earliest opportunity.

(8) Pass instructions to personnel in such a manner as to avoid panic.

(9) Secure classified and/or valuable material before evacuating area. Note that a bomb threat could be used as a screen in order to clear an area prior to attempting to gain unauthorised access.

(10) Establish strict control of all incoming parcels and personal belongings. All personnel effects should be clearly marked with the owners details.

(11) Trained personnel with appropriate equipment should conduct any search. Consideration may be given to involving personnel who have a good working knowledge of the area to be searched.

(12) Do not use lifts/elevators during emergencies.

c. **IED Discovery.** If a bomb or suspected bomb is found on the premises, the local Chain of Command should be alerted at the earliest opportunity. All threats should be reported to the HN security authorities and to the NATO Chain of Command. As part of Response planning, include the additional points:

(1) **Do not touch**; do not immerse in water. If considered safe to do so, obtain a photograph of the device.

(2) Isolate and contain the person(s) who found the device and ensure they are available and prepared to brief the emergency services as soon as they arrive. Obtain a detailed written statement at the earliest safe opportunity.

(3) Do not expose personnel unnecessarily; cordon-off the area and ensure the appropriate NATO and HN security authorities and first responders are notified.

(4) Identify an ERV for the emergency services and have available a number of options to propose as ICPs. It is absolutely essential that all rendezvous points, evacuation areas and ICP locations be checked for any secondary devices before occupation. Remember that a terrorist could well

have observed a training event and know how you are likely to respond.

(5) If not already done so, order evacuation of area, leave windows and doors open. Evacuation routes and assembly area(s) should first be checked to ensure that they are free of any other suspect devices.

(6) Secure classified and/or valuable material in immediate area before evacuation, whenever possible but do not waste time doing so.

(7) If appropriate, safe to do so and practical, shut off any utilities leading into the danger area. Pay particular attention to any gas or fuel lines that may be ruptured in the event of an explosion.

(8) Remove inflammable materials from the area surrounding any device and in the vicinity of any evacuation area.

(9) Place any on-base first responders on immediate readiness.

(10) Since bombs may be detonated by radio transmissions, all Radio Frequency (RF) emitters within a radius of 250m should be shut down.

(11) Ensure evacuated personnel are kept informed and evacuate to cover (particularly in inclement weather) at the earliest opportunity.

(12) Think about possible Strategic Communication issues and control of personal mobile data communications (e.g. accept that it is almost inevitable that someone will post something concerning any emergency evacuation on-line).

(13) Be prepared to assist the emergency with work parties as directed.

d. **IED Detonation / Post Incident Recovery.** If an IED detonates:

(1) Notify the emergency services. Do not assume that this has been done. They would rather receive multiple emergency calls than none at all.

(2) Evacuate personnel from the area affected, after checking first that evacuation routes and assembly points are free from suspect devices.

(3) Start to consider at the earliest opportunity that if there has been a successful bomb attack, another device could well have been planted or another method of follow-up attack might be imminent. Where are the safe areas?

(4) Physically account for personnel and report through the Chain of Command. If appropriate (and in consultation with HN emergency services) consider declaring a Major Medical Incident noting that COM MED may consider declaring a Mass Casualty (MASCAL) incident.

(5) Identify and clear emergency service rendezvous points and ICP. Be prepared to meet and brief emergency services as they arrive. A casualty triage area will be required with access and egress for ambulances. In the case of a MASCAL incident, a temporary morgue facility may be required.

(6) Start to treat casualties if at all possible. Triage and provide first aid until the medical first responders arrive.

(7) Protect classified/valuable material only if safe to do so.

(8) Protect evidence at the scene of the incident until HN security agencies arrive.

(9) Keep personnel informed and control use of personal communications. No one should be allowed to leave without first being accounted for.

(10) Families off-base should be considered. They will want to know what has happened and will demand information at the earliest opportunity.

(11) Be prepared to assist the emergency with work parties as directed.

(12) Implement Major Incident Plan (to include media handling).

(13) Implement Business Continuity Plan. If appropriate, consider transferring responsibility for any ongoing activity under command to an alternate facility.

e. **Postal Bomb Threat.** In this planning phase, the postal (mail) bomb threat is considered to consist of two categories that are differentiated by size, letter-IEDs (including 'book-bombs') and the standard package or IED[24]. Although the extensive use of such devices has been predominantly attributed thus far to very few terrorist groups, it cannot be discounted that such tactics will be copied by other terrorist groups as a technique of terror that offers a reasonably high chance of success, coupled with relatively low-risk for the terrorist, whilst still providing an excellent vehicle for attracting widespread attention to the terrorists' cause. Therefore, commanders need to ensure that their bomb threat plans include provisions for dealing with postal bombs. The following guidance is intended to assist the security officer in developing plans to effectively deal with the threat of postal (mail) bombs:

(1) Appoint a mailroom postal bomb co-coordinator and an alternate.

(2) Establish direct lines of communication between co-coordinator and security officer.

(3) Develop specific screening and inspection procedures for all incoming mail and package deliveries.

(4) Develop specific techniques and procedures to be used by mailroom personnel for handling postal items identified through screening as suspect.

[24] A further threat is posed by suspicious packages that are considered to contain chemical, biological or radiological agents. Advice from Response forces may differ between Installations; consequently contingency planning must be made in consultation with specialist HN agencies to minimize the risk of a successful attack.

(5) If mail is left unsorted for any time after arrival, designate a temporary storage location away from workflow.

(6) Design and construct an isolation area for depositing suspect postal items encountered through the screening process, and establish a minimum safety zone around it. If the screening process (X-ray (fluoroscope)) identifies a postal device, it should not be moved. The area should be evacuated and appropriate HN security agencies notified through the Chain of Command.

(7) Develop identification/verification procedures for postal items encountered through the screening process.

(8) Conduct training sessions with mail-room personnel to ensure complete understanding and practicability of all phases of the postal bomb security plan.

(9) **Screening Procedures.** Items of mail should be treated as suspect if:

(a) The postmark or the name of the sender on the envelope indicates that the letter or package is from an unusual point of origin or sender.

(b) The handwriting on the envelope or package is unfamiliar in style.

(c) The package is ‘lop-sided’ or of uneven balance.

(d) It is of excessive weight for its size. Effective letter bombs usually weigh more than 50 grams (2 ounces).

(e) It is thicker than 5 mm (3/16 in).

(f) There is springiness in the top, bottom or sides.

(g) There is any small pinhole or perforation in the envelope or package.

(h) There are greasy marks on the envelope or package.

(i) There are unusual odours, particularly a smell of almonds or marzipan.

(j) The package makes a noise such as that of a loose piece of metal moving inside.

(k) There is stiffening inside the envelope either with card, or the feel of metal or plastic.

3. **Terrorist Attack.** Additional points in the ISP which are of particular importance in the context of a terrorist attack include, but are not limited to, the following:

a. VIP itineraries to be subject to strict need to know requirements during planning.

b. The provision of Intruder Detector Systems (IDS) with audible alarms for deterrence and/or silent instant internal alarm systems for deterrence and arrest. The reaction time of any response forces will govern this decision.

c. Arrangements to cordon off immediately the area of the incident.

d. Notification of attack to appropriate HN authorities to include nationality of terrorists and languages spoken, if known, and availability of interpreters.

e. Special protection for sensitive areas.

f. At entrances to security zones or sensitive areas, appropriately robust barriers with shatterproof interior panes and proper control of entry for identification should be installed.

g. The potential need to control internal movement of staff.

h. The progressive restriction on vehicle access to a site culminating, where necessary, with total prohibition on vehicles entering or leaving the site at higher Alert States.

i. Emergency arrangements for dealing with casualties.

j. Emergency supplies of food and water to staff marooned by the incident.

k. The provision and issue, where necessary, of bullet-proof clothing to security forces.

The general aim should be to plan to isolate the area of the incident until the assumption of command and control by the HN authorities.

APPENDIX 3 TO
ANNEX F TO
AD 070-001
DATED 22 DEC 21

PROTECTION MEASURES TO BE TAKEN OUTSIDE NATO FACILITIES

1. The following list of precautionary, deterrent and protective measures is neither exhaustive nor universally applicable but it provides a check-list that can be used by security officers, after coordination with the appropriate HN authorities, to give advice on self-protection to prospective kidnap victims or to all staff in high threat areas where terrorism is possible or anti-NATO feeling is high.

a. **At Home:**

(1) Arrange for appropriate protection of the potential target.

(2) Consider evacuating target and the family from danger area as an alternative to providing protection at home.

(3) Keep doors and windows locked and seek advice regarding the installation of appropriate intruder detection systems. Ensure that in securing premises that evacuation in event of fire is not excessively restricted.

(4) Ensure all entry points can be effectively secured with robust locking mechanisms.

(5) Screen against observation from outside. Draw curtains and close any shutters fitted at night.

(6) Keep tight control of house keys. Do not allow duplicates to be made without prior permission. Give out as few keys as possible. Do not label your home keys with your name or address. Have the locks changed in case of doubt.

(7) Reveal no information to strangers calling by telephone; call back to confirm identity or otherwise check. Similarly give no information, particularly concerning dates and times of absence, whereabouts, etc., to a telephone answering service.

(8) Do not advertise employment details, addresses, dates of absences or any other personal information that may be used for targeting purposes. This includes ‘On Line’ activities such as using Social Networking Sites.

(9) In the event of frequent telephone calls from unknown persons who do not speak or who give no valid reason for calling, inform the Chain of Command and HN police.

(10) Avoid setting patterns in personal or family routine to make planning any attack difficult.

(11) Observe the building for a few moments before going in. Notify police if you notice anything unusual. Adequate outdoor lighting is an effective

deterrent.

(12) Instruct members of family and anyone employed around the home (gardeners, cleaners, child minders etc.) on security measures to be taken at home.

(13) Screen domestics, including baby-sitters, before hiring them by submitting their name and date and place of birth through the appropriate agencies at the place of work.

(14) Give clear instructions to domestics not to admit unknown callers and request them not to discuss personal family matters with anyone.

(15) Do not accept gifts from strangers at the door.

b. **When Travelling by Car.** The best protection against attack in a car is the ability to summon help with a mobile phone. Additionally:

(1) Before entering the car, check it for suspicious items or persons.

(2) Keep the bonnet/hood and boot/trunk/luggage compartment locked.

(3) Lock doors not only when parked but also when travelling.

(4) In confined areas and when moving slowly ideally keep windows up but certainly not open more than 5 cm (2 Inches).

(5) Where possible, park cars in a secure and well-lit place.

(6) When exiting a vehicle be aware of anyone watching. Return to vehicles by a different route and do not walk directly to a vehicle. Be alert for the presence of the same people who were in the vicinity at the time of leaving. If it is necessary to check the vehicle for suspicious devices, if possible have someone keep watch as the check is conducted.

(7) Lock the doors and leave the car quickly if it will not start; return only with bona fide assistance or take delivery of it at a garage after it is repaired; do not solicit assistance from passers-by.

(8) Keep fuel levels high. Always have sufficient fuel for your journey and a reserve. Consider carrying spare fuel in an appropriate, approved container.

(9) Cut down on long journeys as much as possible.

(10) Vary routes and timings on regular journeys. Look at other ways of undertaking unavoidably regular journeys like going to work and school runs.

(11) Avoid travelling at night.

(12) Do not stop if signalled by unknown people and do not give lifts to strangers. Only stop if you think there is a problem with your vehicle, not if someone indicates to you there is a problem.

(13) If possible, keep clear of the scene of an accident, a car manoeuvring, or other such situations liable to block your route. Be suspicious if someone hits you unexpectedly. Try to remain calm and if safe to do so, try to keep moving and drive to a safe area, preferably a police station or military base.

(14) Avoid narrow or deserted streets.

(15) Do not get involved with groups gathered in the street, demonstrations, etc., or in arguments with other drivers.

(16) Take evasive action if being followed and drive in the centre lane. If your follower persists, drive to some occupied location and phone for assistance (see (13) above).

(17) If another single vehicle tries to force the car to the side of the road, it may be inadvisable to slow down, even at the risk of an accident.

(18) Plan routes. Find out the location of police stations and armed forces barracks and, when possible, choose a route that passes them.

(19) Keep a look-out to see if the car is being followed; if it is, drive to the nearest police station or military base for assistance.

(20) Instruct office staff of senior officials to be cautious in speaking to unknown persons over the telephone concerning travel arrangements and general whereabouts of officials.

(21) Do not give advance notice of routes to drivers.

(22) Do not keep appointments with unknown persons.

(23) Try to avoid using taxis, but if necessary, take one of those waiting at regular taxi stands. If possible, book with reputable and known companies.

(24) Avoid driving alone.

(25) Avoid travelling in uniform including to and from work.

(26) Remove any insignia / stickers / decals that link private vehicles to NATO or military employment.

c. **When on Foot:**

(1) Keep to well-used streets by day and well-lit streets by night. Avoid shadows and areas such as alleys and doorways that may conceal a threat.

(2) Walk on the side facing oncoming traffic.

(3) If you think you are being followed, enter a public building; use your mobile phone or a public telephone to call for help. If neither is possible, slow down, speed up and reverse direction to make clear to your follower that you are aware of their presence. Avoid instigating a confrontation.

(4) If you walk, run or cycle regularly, vary route and journey timings.

(5) Have a companion, whenever possible.

(6) A pedestrian is vulnerable when entering or leaving their home. Be alert for suspicious activities in that area.

d. **When the Threat is Very High:**

(1) Stay indoors as much as possible.

(2) Do not go out alone.

(3) Where necessary, avoid using easily identifiable or marked official cars. If possible change cars frequently and try to arrange to travel with at least two cars in convoy.

(4) Use the ‘buddy’ system whereby you check with a friend each other's arrivals and departures by telephone and inform the police if either is overdue.

(5) On long journeys, report in by telephone at intervals along the route.

(6) Consider asking for HN police protection.

ANNEX G TO
AD 070-001
DATED 22 DEC 21

SPECIAL LIMITATIONS FOR ACCESS TO NATO NUCLEAR PLANNING DOCUMENTS

1. As provided for in the "Agreement Between the Parties to the North Atlantic Treaty for Co-operation Regarding Atomic information", C-M(64)39, Article VI and the ATOMAL Control Procedures, C-M(68)41(7th revise), Section II, paragraph 29, some ATOMAL information of special security sensitivity will be released to NATO under Special Limitations as designated by the United States of America. Such Special Limitations imposed will be marked on the face of each such document released. The United States of America has elected that certain information released for use by those in NATO Nuclear Planning (NPG) activities will be subject to predetermined limitations.

2. To assist in the ready identification of such documents, to ensure their continued security, to avoid inadvertent intermingling of these documents with others and to maintain a record of recipients of such information, a document cover sheet, including a record of persons who have had access to the information involved, will be affixed to NATO Nuclear Planning documents.

3. The cover sheet shall include the predetermined Special Limitations required for access to sensitive information released for use in NATO Nuclear Planning activities and a record of all persons who have had access to the Special Limitations information disclosed by the document.

4. Special Limitations documents may be transferred between NATO components unless there is a specific prohibition against such transfers included in the prescribing limitations.

5. Requests for dissemination of designated Special Limitations information beyond the restrictions indicated may be submitted to the United States of America in accordance with C-M(68)41(7th revise), Section II, by any receiving component.

6. Records of access will include clearly legible/printed names and signatures of individuals who have received access through either visual or verbal means.

7. In the event that the initial cover sheet showing those who have had access to Special Limitations information is complete, additional cover sheets will be attached as required. Each new sheet will be consecutively numbered so that a continuous record of access is maintained.

8. NATO originated Nuclear Planning documents will be marked as Special Limitations information on the first page of the document and will also have a cover sheet permanently affixed at the time of preparation. Drafts and working papers containing the same information will be treated in the same manner as finished documents.

9. Special Limitations documents do not require separate storage facilities. However, care must be taken to ensure that only persons qualified within the terms of the Special Limitations have access to such documents while in storage, transport, etc.

10. ATOMAL access lists as required by C-M(68)41(7th revise) should include an indication as to those ATOMAL cleared individuals who have been authorised for access

to Special Limitations information.

11. Cover sheets may be requested from the NOS as required. They may be locally reproduced.

ANNEX H TO
AD 070-001
DATED 22 DEC 21

LIST OF THE ATOMAL CENTRAL REGISTRIES WHICH WILL ACT AS CENTRAL CONTROLLING OFFICE FOR THE ATOMAL PROGRAMME IN EACH NATO COMPONENT

1. The responsibility for administering the communication of ATOMAL information in each member state will be performed by the agencies designated below:

Belgium

Central Registry Belgian Defence
Staff Department Operations and Training
Division Operations
Office du Contrôle Atomique Belge - OCABE (B)
Queen Elisabeth Barracks – Building 1
Everestraat 1, 1140 Brussels – Belgium
Phone: +32 2 44 17100
Fax: +32 2 44 39647
Cell: +32 473 79 31 83
E-mail: BELJOINTDCACO-CentralRegistry@joint.mil.be
NNCCRS: MOD BE

Bulgaria

COSMIC and ATOMAL Central Registry
State Commission for Information Security (SA)
No.1 “Angel Kanchev” Str.
SOFIA 1040
Phone: +359 2 921 5911
Fax: +359 2 987 3750
E-mail: dksi@government.bg

Canada

Department of National Defence
ATOMAL Control Officer
National Defence Headquarters
Ottawa, Ontario
K1A OK2 - Canada
Telegraphic address: NDHQ – OTTAWA

Czech Republic

Central COSMIC and ATOMAL Registry
National Security Authority
NBÚ (SA)
Na Popelce 2/16
150 06 Praha 56, Czech Republic
Phone: +420 257 28 33 49
Fax: +420 257 28 32 10
E-mail: ust.registr@nbu.cz

AD 070-001

Denmark

Ministry of Defence
Service and Administration
ATOMAL Control Office
Holmens Kanal 42
DK – 1060 Copenhagen K.
Phone: +45 72 81 00 00
Fax: +45 72 81 03 00
E-mail: fmn@fmn.dk

Estonia

Estonian Information Board
National Security Authority Department
ATOMAL Central Registry
Rahumäe tee 4B
11316 Tallinn
Estonia
Phone: +372 693 9211
Fax: + 372 693 5001
E-mail: nsa@teabeamet.ee

France

Chef du Bureau central COSMIC/ATOMAL
Service de Sécurité de Défense
Secrétariat Général de la Défense nationale
51 Bd de Latour Maubourg
75700 Paris - France
Telegraphic address: MOD FRANCE

Germany

Minister of Defence
COSMIC and ATOMAL Central Agency
of Federal Republic of Germany
Stauffenbergstrasse 18
D-11055 Berlin
Phone: +49 (0)1888 24 2116
Fax: +49 (0) 1888 24 8320
E-mail: bmvgorgberlin@bmvg.Bund400.de
Telegraphic address: MOD GERMANY Berlin

Greece

ATOMAL Central Registry
Hellenic National Defence General Staff
HND6S Building
Holargos - Athens
Telegraphic address: ATOMAL Central Registry – HND6S

Hungary

COSMIC and ATOMAL Central Registry
Ministry of Defence
MOD Hungary

Balaton street 7-11
H1055 Budapest
Phone: +36 1 346 9652
Fax: +36 1 346 9658

Iceland

Ministry of Foreign Affairs
Reykjavik

Italy

Presidency of Council of Ministers
National Security Authority
Central Security Office
ATOMAL Central Registry
Rome
Telegraphic address: MOD ITALY - ANS-UCSI

Latvia

ATOMAL Central Registry
National Security Agency
Constitution Protection Bureau
Miera iela 85a
Riga, LV – 1013, Latvia
Phone: +371 702 5471
Fax: +371 702 5406
E-mail: info@sab.gov.lv

Lithuania

ATOMAL Central registry
Ministry of National Defence
Totoriu str. 25/3, Vilnius, Lithuania
Phone: +370 5 2735 546
Fax: +370 5 2735 544

Luxembourg

Le Gouvernement du Grand-Duché de Luxembourg
Ministère d'État
Centre de Communication du Gouvernement
Bureau d'Ordre Central – COSMIC et ATOMAL
Château de Senningen
L-6961 Senningen, Luxembourg
Phone: +352 478 7122
Fax: +352 478 7234
E-mail: boc@ccg.etat.lu

Netherlands

Ministry of Defence
Chief Defence Staff
Room A 210
Plain 4 - The Hague
Telegraphic address: MOD NETHERLANDS – CDS

Norway

Royal Norwegian Ministry of Defence
Cosmic and ATOMAL Central Registry
P.O. Box 8126 Dep
0032 Oslo

Norway

Visitor address: Glacisgata 1, 0150 Oslo
E-mail (unclassified): postmottak@fd.dep.no
Phone CACO: +47 23 09 6163/6299
Telegraphic address: MOD NORWAY

Poland

Central ATOMAL Registry
(CTS/A in military sphere)
Military Information Services – WSI/SA
Al. Niepodleglosci 241/243
00-909 WARSZAWA 60, Poland
Phone: +48 22 6841 584
Fax: +48 22 6874 118

Portugal

Presidency of the Council of Ministers
National Security Cabinet
ATOMAL Central Registry
Av. Ilha da Madeira n.1
1400-204 Lisboa, Portugal
Phone: +351 213 041 820
Fax: +351 213 031 711
E-mail: gns@netcabo.pt

Romania

COSMIC and ATOMAL Central Registry
National Registry Office for Classified Information
(O.R.N.I.S.S.)
Mures Street 4
Bucharest, Sector 1, Romania
Phone: +40 021 2075110
Fax: +40 021 2242801
E-mail: nsa.romania@orniss.ro

Slovakia

National Security Authority
COSMIC and ATOMAL Central Register
Budatínska 30
P.O. BOX 16
850 07 Bratislava 57
Slovak Republic
Phone: + 421 2 6869 2527
E-mail: sknsareg@mod.sk.nato.int

AD 070-001

Slovenia

Ministry of Defence
Centralní register
Vojkova 55
1000 Ljubljana
Slovenia
Phone: +386 1 230 53 56
Fax: +386 230 52 44

Spain

ATOMAL Central Registry
Avda. Padre Huidobro s/n
28023 Madrid
Spain
Phone: +34 91 372 5709
Fax: +34 91 372 5808
E-mail: asip@areatec.com

Turkey

Republic of Turkey
Headquarters Turkish General Staff
ATOMAL Central Registry
TGS
MUSAT
Ankara
Turkey
Telegraphic address: MOD TURKEY

United Kingdom

a. DI PR-Sy IDR 1
Room 40D
Old War Office Building,
London SW1A 2EU

b. UK authority responsible for overall control and transmission of UK ATOMIC information and contact point for routine questions and requests:

DG Strat Tech, ATOMIC CONTROL OFFICE (London)
Ministry of Defence,
Main Building, Whitehall, London, SW1A 2EU

The following are specific questions and requests to be referred to AD/Sc(Nuc)2/ATOMIC CONTROL OFFICE:

(1) requests for UK ATOMIC information;

(2) questions regarding content and classification of documents containing UK ATOMIC information;

(3) modification of Special Limitations;

(4) reports of compromises of UK ATOMIC information.

AD 070-001

United States

a. Central ATOMAL Registry
Central U.S. Registry, Room 1J664A
The Pentagon
Washington, D.C. 20310
Telegraphic address: SECDEF WASHINGTON

b. United States initial point-of-contact for all questions concerning United States policy pertaining to the ATOMAL Agreement and this document:
US Mission to NATO

c. Annual muster reports (per Section III, Para. 60 herein) and inspection reports (per Section III, Para. 61 to 66):
Central U.S. Registry, as in (1) above.

d. US Agency responsible for supervising initial releases of ATOMAL information and point-of-contact for related questions and requests arising under the Administrative Arrangements to Implement the ATOMAL Agreement:

Joint Atomic Information Exchange Group
8725 John J. Kingman Road
Mail Stop 6201
Ft. Belvoir, VA 22060-6201
(an information copy of each communication to JAIEG should be provided to the US Delegation at NATO Headquarters).

The following are specific questions and requests to be referred to JAIEG:

(1) modification of Special Limitations (Section II, paragraph 29, ATOMAL Control Arrangements);

(2) reproduction of documents (Section III, paragraphs 47 and 49, ATOMAL Control Arrangements);

(3) requests for Restricted Data and Formerly Restricted Data (Section II, paragraph 19, ATOMAL Control Arrangements).

e. US authority responsible for ATOMAL content and classification of ATOMAL information (Section III, paragraphs 38 to 42 herein):

United States Security Authority for NATO Affairs
Director, International Security Programs
ODUSD (Technology Security Policy & Counter-Proliferation)
Room 1E814 Under Secretary of Defense (Policy)
Washington, D.C. 20301-2200

A copy of all correspondence will also be forwarded to the:

Director
Office of Classification, US Department of Energy
DP-32, Washington, D.C. 20545

2. These responsibilities for NATO international Civil and Military Organisations will be performed by the agencies as designated below:

a. North Atlantic Council
ATOMAL Central Registry
NATO Headquarters
1110 Brussels, Belgium

b. The Military Committee
ATOMAL Central Registry
International Military Staff Military Committee (IMS-MS)
NATO Headquarters
1110 Brussels, Belgium

c. Allied Command Operations (ACO)
Attn: ACO COSMIC and ATOMAL Control Officer
B-7010 Casteau, Belgium

d. North Atlantic Treaty Organisation
Headquarters, Supreme Allied Commander Transformation
Attn: ATOMAL Control Officer
7857 Blandy Road, Suite 100
Norfolk, Virginia 23511-2490, USA

3. A NATO component may change its administrative agency upon notification to the NATO Office of Security and to all other ATOMAL Central Registries listed at paragraphs 1 and 2 above.

ANNEX I TO
AD 70-001
DATED 22 DEC 21

COVER SHEET FOR ATOMAL DOCUMENTS

Subject	Control Number(s)	Enclosure(s)

The attached document contains information, the security aspect of which is paramount, and unauthorised disclosure of which would cause grave damage to NATO. Special care in the handling, custody, and storage of the attached information must be exercised in accordance with the NATO ATOMAL security regulations. This cover sheet is **NOT A RECEIPT** but a record of persons who have had access to the document(s) identified by number above.

Each person receiving the attached document shall sign and fill in the information required below.

		DATE	REMARKS
	NAME	RECEIVED RELEASED	(Indicated portions and all of documents read)
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

THIS COVER SHEET SHALL NOT BE REMOVED UNTIL DESTRUCTION OF THE ATTACHMENT AT WHICH TIME IT WILL BECOME NATO CONFIDENTIAL AND BE RETAINED FOR TEN YEARS IF THE ATTACHMENT WAS COSMIC TOP SECRET ATOMAL AND FOR FIVE YEARS IF THE ATTACHMENT WAS NATO SECRET ATOMAL OR NATO CONFIDENTIAL ATOMAL.

AD 070-001

COVER SHEET

FOR SPECIAL LIMITATIONS INFORMATION DISSEMINATION LIMITED BY THE UNITED STATES OF AMERICA

As stated in the "Agreement Between the Parties to the North Atlantic Treaty for Cooperation Regarding Atomic Information" and in the ATOMAL control arrangements, special limitations may be prescribed by the United States on communication of ATOMAL information. The Government of the USA has determined that certain information furnished for use by those in NATO nuclear planning activities will be subject to the following special limitations, in addition to those specified in the ATOMAL control arrangement.

Access

Access to documents so marked is limited to personnel meeting all of the following requirements:

1. Have been granted an appropriate NATO security clearance for access to ATOMAL information;

2. Have been determined by a responsible official within the component to have a need-to- know for NATO nuclear planning activities such as those performed by the Nuclear Planning Group (NPG);

3. Have been individually approved by the component security authority and have had their names placed on their Security Authority's list of approved recipients for such information.

4. Occupy one of following positions:

   a. Chiefs of State, Heads of Government, and such ministers and heads of Government departments or agencies as have responsibilities for NATO nuclear planning matters and a limited number of advisors on such matters to each of these officials;

   b. Permanent Representatives to the NAC, if NATO nuclear planning responsibilities are entailed, and such members of their delegations as have such responsibilities;

   c. The SEC GEN and such other members of the International Staff as have responsibilities for NATO nuclear planning matters;

   d. Members of the Military Committee and a limited number of staff officials who advise the Committee on NATO nuclear planning matters;

   e. The NATO Defense Planning Committee; the NPG; a limited number of staff officers who advise these committees on such matters ; and, such members of these committees' working groups and technical panels as require access to the information;

   f. Commanders of NATO Strategic Commands (ACO and ACT) and a limited number of such a commander's staff who are advisors on NATO nuclear planning

matters;

g. Personnel of members states and NATO military commands who participate in the nuclear planning work and studies of the committee or groups established by the North Atlantic Council and require access in connection with that participation;

h. ATOMAL Control officers and alternates and minimum administrative personnel who must handle the information in order to support the other personnel designated.

ANNEX J TO
AD 070-001
DATED 22 DEC 21

REQUESTS FOR ATOMAL INFORMATION

1. Requests for ATOMAL information to the Government of the United States of America or to other NATO components should be transmitted consistent with Annex H and be submitted in writing to the Joint Atomic Information Exchange Group. The following information shall be included:

a. A description of the information required;

b. Statement of the purpose for which the information is required and the desired dissemination;

c. Number of copies required;

d. Any other pertinent information which will assist in processing the request.

2. Requests for UK ATOMIC information shall be addressed in writing to DG Strat Tech, ATOMIC CONTROL OFFICE (London), Ministry of Defence, Main Building, Whitehall, London, SW1A2HB through the official UK Representative at NATO civil and military organisations and will include all the elements listed in the preceding paragraph.

3. **VISITS.** Visits between NATO components involving ATOMAL information should be preceded by a written request to the NATO component to be visited, transmitted consistent with Annex H. The request should include the following:

a. Name and location of the activity to be visited and, If known, the specific individual to be contacted;

b. Proposed dates for the visit;

c. Purpose of the visit;

d. Name and security clearance of each visitor;

e. A statement that each visitor has a need-to-know the information involved.

ANNEX K TO
AD 070-001
DATED 22 DEC 21

METHODS AND CRITERIA FOR DESTRUCTION

1. Hammer mills, pulping machines and shredders destroy the classified material with varying degrees of effectiveness according to the type and mechanical condition of the equipment but the problem of final disposal of the bulk remains (sewage systems, bags or hoppers). Burning is a positive and complete method of destruction and there is very little fine ash left in proportion to the volume burned. The following are general equipment requirements:

a. **Shredding Machines.** Shredding machines used to destroy classified material in accordance with the requirements of Paragraph III-104., must have a cut of 0.8 mm (maximum 1.5 mm) wide and a cross-cut of 12.5 mm (maximum 20 mm) in length. Shredders must be constructed so that material cannot be left undestroyed in the machine after the operation.

b. **Pulpers and Disintegrators.** The machine must grind classified waste material by breaking down the fibre resistance. The pulped matter must be disintegrated and de- fibred so as to be incapable of reconstruction as recognisable information. An approved security locking device capable of being fastened with double padlocks is to be provided to cover the loading head or any other aperture giving access to the inside of the tank.

c. **Incinerators.** Incinerators are to be constructed to accept classified waste in standard sealed bags. Any aperture that permits access to classified waste or ash during or after combustion must be sealed or padlocked. The ash residue must not be recognisable as readable matter.

d. **Guidance.** Host nation requirements are to be met for the standards of destruction machinery and methods. Additionally, local elements of supporting CI agencies will provide guidance on approved shredding machines and will, on request, evaluate specific models to ensure they comply with national and NATO standards.

e. **Crypto Material.** Specific standards for destruction of classified crypto material are contained in ACO Directive (AD) 090-009.

ANNEX L TO
AD 070-001
DATED 22 DEC 21

DISPOSAL AND DESTRUCTION OF CLASSIFIED MAGNETIC MEDIA

1. Magnetic storage media containing classified information shall not be disposed of or released to environments outside of ACO but shall be destroyed. Those persons charged with maintaining the security of information shall ensure that magnetic media is adequately destroyed. Records of destruction will be maintained in accordance with ACO policy. As there are no standard means available for the disposal and destruction of classified magnetic media, individual ACO Commanders are responsible to arrange for the disposal and destruction of classified magnetic media, in accordance with the policies below.

2. **Determining Adequate Destruction.** The decision that magnetic storage media is adequately destroyed rests with the destroyer. The destroyer shall base that decision on having employed the recommended destruction method and having considered the threat and all other conceivable factors affecting the risk. Approved and recommended destruction methods on CIS Storage Media related to the classification level of the respective items and the local security environment are detailed in AD 070-005. The adequacy of destruction requires witness concurrence.

3. **Disposal of Destroyed Classified Magnetic Media.** Once magnetic storage media that had contained sensitive information is adequately destroyed, it shall be treated as normal waste. Waste disposal shall conform to host country environmental regulations.

4. **Destruction Methods.** To properly destroy magnet storage media, the full face of the media memory surface shall be removed/destroyed. Magnetic storage media should be destroyed by one of the following methods:

a. **Disintegration.** Reduces media to particles of sufficiently small size that, in the opinion of the destroyer, the risk of information recovery or reconstruction is acceptably low. Mixing particles of different disintegrated media further reduces the risk.

b. **Pulverising.** Demolishes, crushes or smashes magnetic storage media. Pulverising shall be to such an extent that, in the opinion of the destroyer, the risk of information recovery or reconstruction for the purpose of exploitation is acceptably low.

c. **Melting.** Exposing the magnetic media to extreme heat to such an extent that the media softens or liquefies and that, in the opinion of the destroyer, the risk of information recovery or reconstruction is acceptably low.

d. **Shredding.** Is an acceptable method of destroying magnetic tapes, floppy disks, diskettes and other magnetic storage devices having similar flexible platters. Media shall be removed from their encasings before shredding. When shredding magnetic storage media, the security requirement for the cutting characteristics of the shredder must meet the same requirements as for sensitive paper copy.

e. **Burning.** Incinerators are to be constructed to accept classified waste in standard sealed bags. Any aperture, which permits access to classified waste or ash during or after combustion, must be sealed or padlocked. The ash residue must not be recognisable as readable matter.

5. **Preparation Requirements for Destruction by Disintegration.** Magnetic storage media is subject to the following rules prior to disintegration:

(1) COSMIC TOP SECRET information shall be purged prior to media disintegration.

(2) NATO SECRET information **shall be purged** prior to media disintegration.

(3) NATO CONFIDENTIAL information **should be purged** prior to media disintegration.

(4) NATO RESTRICTED information needs not be sanitised prior to destruction by disintegration.

6. **Disintegration Procedure.** Use the disintegrator according to the manufacturers' directions. Disintegrating media of different classifications at the same time is recommended. If not mixed during disintegration, the disintegration particles should be intermixed with those of other classifications levels after disintegration.

7. **Pulverising Magnetic Storage Media.** Pulverising is recommended for magnetic drums, core memory of relatively large size and sensitive CIS hardware for which no other method is practicable.

8. **Pulverising Prerequisites.** All magnetic storage media containing or suspected of having contained information classified NATO SECRET and higher shall be purged prior to destruction by pulverising.

9. **Adequacy of Pulverising.** Those persons destroying the media shall exercise judgement that the media is adequately pulverised. The person destroying the media shall be familiar with the techniques and shall be knowledgeable of the media being destroyed. Where the media is not reduced to dust or sufficiently small particles, the destroyer shall ensure that the total media surface has been adequately struck. Witnessing is required in all cases where commercial private sector pulverisers are used on magnetic media containing or having contained classified information.

10. **Methods of Pulverising.** Extreme care must be exercised when pulverising magnetic media. Information is removed from the media only at the points where the pulveriser impacts the media. Therefore, media must be pulverised until, in the opinion of the destroyer and witness, the particles are sufficiently small or powdered or that the total surface of the media has been struck. Due to there being no authorised facilities to pulverise magnetic storage media, the following are some methods that may be used to destroy media:

a. Commercial car crushers.

b. Metal presses.

c. Where media and hardware are sufficiently small, they may be beaten with a hammer.

11. **Melting Magnetic Storage Media.** Melting, dissolving or similarly altering the physical state of the media is acceptable for destroying all types of magnetic media. The requirement for records and certificates of destruction shall be in accordance with ACO policy.

12. **Melting Prerequisites.** All magnetic storage media containing or suspected of having contained classified information should be purged prior to destruction by melting. The person destroying the media shall be familiar with the techniques and shall be knowledgeable of the media being destroyed.

13. **Adequacy of Melting.** As with other destruction processes, those persons charged with destruction shall exercise judgement that the media is adequately melted or decomposed to deny any access to the information. The adequacy of destruction requires witness concurrence.

14. **Methods of Melting.** There are no known facilities dedicated to melting magnetic storage media. The following are some methods that may be used to melt or dissolve media: Applying open flame such as a welding torch, dry acid or other corrosive chemical given the following stipulations:

a. The media is in a container able to withstand the required heat.

b. The area is ventilated according to host country safety standards.

c. The media being melted does not begin to burn or produce harmful environmental toxins.

15. **Shredding Magnetic Storage Media.** Shredding is acceptable for destroying magnetic tapes, floppy disks, diskettes and other magnetic storage devices having similar flexible platters. The requirement for records and certificates of destruction apply in accordance with ACO policy.

16. **Shredding Considerations.** Magnetic storage media containing information classified NATO SECRET and above shall be purged prior to destruction by shredding. The security requirement for the cutting characteristics of the shredder must meet and shall be commensurate with the standards for the highest sensitivity level of information ever held on that media. Magnetic storage media shall be removed from their containers prior to shredding.

17. **Adequacy of Shredding.** Those persons charged with destruction shall exercise judgement that the media is adequately shredded to deny any access to the information contained on the destroyed media. The person destroying the media shall be familiar with the techniques and shall be knowledgeable of the media being destroyed. The adequacy of destruction, depending on the sensitivity of information, may require witness concurrence.

18. **Shredding Criteria.** Shredders must have a cut of 0.8 mm (maximum 1.5 mm) wide and a cross-cut of 12.5 mm (maximum 20 mm) in length. Shredders must be constructed so that material cannot be left undestroyed in the machine after the operation.

19. **Crypto Material.** Specific standards for destruction of classified crypto material are contained in ACO Directive (AD) 090-009.

ANNEX M TO
AD 070-001
DATED 22 DEC 21

SECURITY ASSURANCE

The Non-NATO Nation or Organisation:

……
(name of non-NATO Nation or Organisation)

Representative of the Non-NATO Nation or Organisation:

……
(printed name and title of individual, and signature of individual)[25]

For the purposes of, and participation in:

……
(name of the NATO activity)

The Non-NATO Nation or Organisation hereby agrees:

(a) To protect NATO Classified Information provided to it by …….. (*name of the NATO activity*) in accordance with the Annex[26] to this Assurance;

(b) To provide such classified information only to appropriately cleared individuals under its jurisdiction with a need-to-know;

(c) To use such information only for the purposes for which it was provided to it;

(d) Not to transfer such information to a third party without the prior written consent of the originator of the information;

(e) To continue to abide by the security requirements of the Annex to this Assurance even after completion of ……(*name of the NATO activity*);

(f) That this assurance will terminate upon the conclusion of the …….. (*name of the NATO activity*) and that it will be re-validated every 6 months with the NATO Office of Security.

[25] The signatory is an officially authorized representative who is either the direct recipient of released information or is a senior representative responsible for ensuring the protection of information released in support of a co-operative activity.
[26] Refers to Appendix 1 to this Annex.

APPENDIX 1 TO
ANNEX M TO
AD 070-001
DATED 22 DEC 21

MINIMUM STANDARDS FOR THE PROTECTION OF NATO/*(NAC-approved activity or NPLO activity)* CLASSIFIED INFORMATION FOR *(applicable Non-NATO Entity)*

Security Clearance and Authorisation for Access

1. Before an individual is granted access to NATO/(*NAC-approved activity or NPLO activity)* Classified Information, they will be subject to a security clearance procedure designed to determine whether the individual is loyal, reliable and trustworthy, by considering the individual aspects of character and circumstances which may give rise to potential security concerns.

2. These elements shall be assessed, in accordance with national laws and regulations, to determine if the individual can be associated with any activity related to espionage, terrorism, sabotage, treason, sedition, subversion, crime, or behave in a manner which could potential make them vulnerable to blackmail or pressure.

3. When the result of a security clearance procedure is positive, the recipient nation/organisation is to produce a Personnel Security Clearance (PSC) Confirmation in accordance with the format at the Tab A[27] to this Appendix 1 to Annex M, which is to be forwarded to the appropriate Security Authority.

4. Upon receipt of the PSC Confirmation, the appropriate Security Authority will authorise access to information and areas, in accordance with the individual's need-to-know.

5. The individual shall be briefed by the appropriate Security Authority on the security regulations relevant to the classification of the information to which they will be granted access.

Definitions of Security Classification Markings

6. The security classifications are used to indicate the sensitivity of classified information and thus to establish procedures, which shall apply for its protection and handling. The non-NATO recipient shall identify the equivalent security classifications to the NATO security classifications.

Security Classifications	
NATO	**Applicable Non-NATO Entity**
NATO SECRET	
NATO CONFIDENTIAL	
NATO RESTRICTED	

[27] Refers to Appendix 2 to this Annex.

7. The following principles apply to the security classification of NATO/(*NAC-approved activity or NPLO activity)* classified information:

a. NATO/(*NAC-approved activity or NPLO activity*) SECRET. The unauthorised disclosure of which would result in grave damage to the NATO and (*Applicable Nation or Organisation)* mission;

b. NATO/(*NAC-approved activity or NPLO activity*) CONFIDENTIAL. The unauthorised disclosure of which would be damaging to the NATO and (*Applicable Nation or Organisation)* mission;

c. NATO/(*NAC-approved activity or NPLO activity)* RESTRICTED. The unauthorised disclosure of which would be detrimental to the interests or effectiveness of the NATO and (*Applicable Nation or Organisation)* mission.

Requirements for Receipt, Handling, Storage and Passing On of NATO/(NAC-approved activity or NPLO activity) Classified Information

8. **Receipt/Registration.** A Registry system shall be established by the recipient for the receipt, dispatch, control and storage of NATO classified information.[28] Sub-registries may be established as necessary. Registries shall be responsible for:

a. the recording of the receipt and dispatch of all NATO/(*NAC-approved activity or NPLO activity)* classified information.

b. the distribution and control of all NATO/(*NAC-approved activity or NPLO activity*) classified information within the nation/organisation served;

c. the storage and final disposal of all NATO/(*NAC-approved activity or NPLO activity*) classified information which must include:

(1) destruction certificates for all information classified NATO/(*NAC-approved activity or NPLO activity*) SECRET;

(2) logbooks and registers for all information classified NATO/(*NAC-approved activity or NPLO activity*) RESTRICTED or CONFIDENTIAL/

9. **Handling, Storage and Passing On.** The following rules and regulations apply for the handling, storage and passing on of NATO/(*NAC-approved activity or NPLO activity*) classified information:

a. **NATO/(NAC-approved activity or NPLO activity) SECRET.**

(1) NATO/(*NAC-approved activity or NPLO activity*) SECRET information shall be handled, displayed, processed and stored in areas to which access is strictly controlled. Access shall be limited to designated, appropriately cleared individuals with an established need-to-know for official purposes. NATO/(*NAC-approved activity or NPLO activity*) SECRET information shall be stored in security containers with nationally-approved locks, the keys or

[28] The NOS may, subject to certification process, impose more or less stringent requirements with regard to NATO Classified Information requiring registry system control.

combinations to which shall be held only by designated, security cleared personnel, who require access to the stored information in order to fulfil their official duties. Transfer of documents must be made by official courier or diplomatic bag.

(2) Copies of classified information are not to be made without prior authorisation from (*Applicable Nation or Organisation)* HQ J2 Chief/Head of Security Office. If authorised, copies of NATO/(*NAC-approved activity or NPLO activity*) SECRET may only be released to appropriately cleared individuals and only on strict observation of the need-to-know principle. Copies of documents classified NATO/(*NAC-approved activity or NPLO activity*) SECRET must be marked with identifying reproduction copy numbers and must be recorded by the registry (or sub-registry).

b. **NATO/(*NAC-approved activity or NPLO activity*) CONFIDENTIAL**

(1) NATO/(*NAC-approved activity or NPLO activity*) CONFIDENTIAL information shall be handled displayed, processed and stored in areas to which access is strictly controlled. Access shall be restricted to designated individuals who have been appropriately cleared and have an established need-to-know for official purposes. Information shall be stored in security containers with nationally approved locks, the keys or combinations to which shall be held by designated security personnel. Transfer of documents must be by official courier or diplomatic bag. Copies of classified information are not to be made without prior authorisation from (*Applicable Nation or Organisation)* HQ J2 Chief/Head of Security Office. If authorised, copies of NATO/(*NAC-approved activity or NPLO activity*) CONFIDENTIAL may only be released to appropriately cleared individuals and only on strict observation of the need to know principle.

c. **NATO/(*NAC-approved activity or NPLO activity*) RESTRICTED**

(1) NATO/(*NAC-approved activity or NPLO activity*) RESTRICTED information shall be handled, displayed, processed and stored in a manner that deters unauthorised access; for example, in a locked desk, cabinet or room to which access is controlled. Copies of classified information are not to be made without prior authorisation from (*Applicable Nation or Organisation*) HQ J2 Chief/Head of Security office. If authorised, copies of NATO/(*NAC-approved activity or NPLO activity*) RESTRICTED may only be released to appropriately cleared individuals and only on strict observation of the need-to-know principle.

10. **Destruction and Disposal.** Classified information which is no longer required for official purposes, including surplus or superseded information and waste, shall be destroyed in such a manner as to ensure that it cannot be reconstructed.

11. The destruction of information classified NATO/(*NAC-approved activity or NPLO activity*) SECRET is to be recorded. The record is to be signed by the destruction official and an independent witness, both of whom shall be appropriately cleared and authorised to have access to NATO/(*NAC-approved activity or NPLO activity*) SECRET information. Destruction certificates and control records for information classified NATO/(*NAC-approved activity or NPLO activity*) SECRET are to be retained in the registry or office

performing the destruction for a period of not less than 5 years.

Handling of NATO Classified Information on Non-NATO Communication and Information Systems (CIS)

12. If handling of NATO Classified Information on an NNE's CIS is considered a legitimate operational requirement by the NATO body of NATO Nations supporting the activity, this Assurance shall be amended to include specific security requirements for the protection of the subject CIS. Moreover, the NOS approval shall be sought.

Breaches or Compromises of Security

13. Whenever a breach or compromise of security affecting classified documents is discovered, an initial report giving details of the breach/compromise must be sent immediately to (*Applicable Nation or Organisation*) HQ Security Officer. An investigation into the circumstances of the breach/compromise must be carried out immediately in conjunction with (*Applicable Nation or Organisation*) HQ Security Officer and a full report is to be sent to the NOS. At the conclusion of this investigation, remedial or corrective action, where appropriate, shall be taken and the NOS notified. In all cases, the originator will be informed by the NOS.

14. The initial breach/compromise report is to contain the following information:

a. a description of the information involved, including its security classification, marking reference, copy number, date, originator, subject and scope;

b. a brief description of the circumstances of the compromise, including the date, the period during which the information was exposed to compromise; and

c. if known, the number and/or category or unauthorised individuals who have or could have had access to the document.

Security Surveys

The Government/Organisation ……..…….. will facilitate periodic Surveys by NOS (or Delegated Authorities) to ensure that the security arrangements for the protection of the released classified information meet the minimum established standards.

TAB:

A. Personnel Security Clearance Confirmation.

TAB A TO
APPENDIX 1 TO
ANNEX M TO
AD 070-001
DATED 22 DEC 21

PERSONNEL SECURITY CLEARANCE CONFIRMATION
(for non-NATO citizen on the basis of a Security Assurance)

Full Name (LAST NAME, Middle Name(s), First Name):

.....

Title/Rank:

.....

Date and Place of Birth (DD/MM/YYYY, City, Country)

.....

in accordance with national laws and/or applicable security rules and regulations as well as in compliance with the provisions of the Security Assurance for (*name of NAC-approved activity or NPLO activity)* signed by

.....

(*the Government of/name of Organisation)*

has been authorised to have security clearance by:

.....

(*the Government of/name of Organisation)*

has been brief on the security regulations for the protection of NATO Classified Information and the legal and disciplinary consequences of infraction/breaches of those regulations, and is, therefore, declared suitable to be entrusted with information classified up to and including:

NATO/(*NAC-approved activity or NPLO activity*)
SECRET/CONFIDENTIAL/RESTRICTED[29]

The validity of this certificate will expire no later than: (DD/MM/YYYY) __/__/____

Confirming Authority

Name: .....
.....
.....
Phone Number:.....
Email: .....

Date: (DD/MM/YYYY) __/__/____ Signature and Stamp .....

[29] Deleted as appropriate.
(*) The marking is not part of the template.

ANNEX N TO
AD 070-001
DATED 22 DEC 21

GENERAL PROCEDURES FOR RELEASE OF NATO CLASSIFIED AND UNCLASSIFIED INFORMATION TO NON-NATO RECIPIENTS

1. **Requests for Release of NATO Information.** Requests for release shall be sent to the relevant addressee as follows:

a. The NAC Secretariat, NATO International Staff, for NCI issued by the NAC.

b. The Secretary of the appropriate subject-matter committee for information classified up to and including NS, which has been originated by that committee and/or bodies subordinate to it.

c. The Director International Military Staff, for NCI issued by the NAMILCOM and/or bodies subordinate to it.

d. SACEUR or DSACEUR for information classified up to and including NS, which is identified as being releasable to xFOR, or is classified NATO/xFOR SECRET (mission SECRET).

e. The Mission Commander for a NAC-approved operation involving non-NATO Troop Contributing Nations, for information classified up to and including NS that has already been determined as releasable to the mission (xFOR).

f. The Head of NATO Production and Logistics Organisation (NPLO), for NCI originated by and belonging to one or more of the nations participating in the NPLO.

2. **Requests for Release Shall Include the Following Information**

a. For NAC-approved cooperative activities, where potential non-NATO participants to that activity have also been endorsed by the NAC on a case-by-case basis:

(1) Reference to the relevant subject in the overall work plan or the OPLAN for the cooperative activity.

(2) Purpose and justification for the release (initiating co-operation, progress in cooperation, exercise, etc.).

(3) Identification of document(s) containing the NCI (reference number, date and NATO classification).

(4) Description of the NCI, which should be released (the whole document(s), part of the document, or an excerpt from the document).

(5) If appropriate, a request for generic release (i.e. specific subject areas, defined series of documents, anticipated future documents or series of documents, etc., stating maximum classification and any other limitations regarding the possible future release).

b. For releases outside cooperative activities approved by the NAC, the

document containing the NCI must be identified and the information requested in a. (2), (3) and (4) above must be given. Generic release is not authorised.

3. **Actions upon the Receipt of a Release Request.** Addresses receiving a request for release of NCI shall ensure that:

a. The justification given in the release request is adequate.

b. The NCI concerned is properly identified and described.

c. A Security Agreement has been concluded between NATO and the non-NATO recipient, and that the required security survey has been carried out by the NOS with a positive result; or in exceptional circumstances, in order to support specific operational requirements endorsed by the NAMILCOM/NAC (for example, in support of force protection, and the exchange of information), a Security Assurance (see Annex M) from the non-NATO recipient has been provided; or the non-NATO recipient has provided, through its NATO Sponsor, a written Security Assurance to NATO that it will protect NCI of an equivalent classification; or the NATO sponsor has provided the necessary assurance that the appropriate security system is in place in the non-NATO recipient for the protection of released information.

d. The request is sent to the appropriate committee or delegated authority for a decision.

e. Any international organisation, which requests release, has a Security Agreement in force with NATO; and the release of information to its non-NATO members is in accordance with relevant provisions of the Security Agreement, as well as other established rules concerning their participation in NATO activities.

ACTIONS BY THE RELEASE AUTHORITY

4. Based on the information contained in the request, the Release Authority will approve or refuse the release.

5. National members of the Release Authority are responsible for obtaining any approval, which may be required from their national authorities.

6. The Release Authority is responsible for ensuring that any information released to a non- NATO recipient has been reviewed / sanitised, so that the non-NATO recipient is only given information for which he has a requirement / need-to-know.

7. Approval, whether obtained in committee or under the silence procedure, will be recorded in writing.

8. In the context of NAC-approved co-operative activities, the Release Authority may approve generic release of NCI, issued under its authority. Such approval must state the specific subject areas or series of documents containing NCI and the level of classification authorised for release; furthermore, the Release Authority may stipulate any other limitations regarding possible future release.

9. Should a request for release of NCI not be approved by a delegated Release

Authority, the request together with the latter's reason for not approving it, may be presented to the next level and ultimately to the NAC for a final decision. This action will only be taken in cases when sought by the requesting NATO member nation(s), or NATO body, or when the delegated Release Authority decides that such action is appropriate.

MARKING INFORMATION TO BE RELEASED

10. The following procedures shall be used for marking NCI:

a. For existing NATO information: classified information originating from NATO, which is released to non-NATO recipients, shall retain its NATO classification. In addition, the cover or first page of the copy of any document released, and the archive copy, shall be marked with the name of the Release Authority, the date the release decision was taken, and any related terms or conditions.

b. For NATO information created within NAC-approved activities, where the designation of an activity marking has also been approved by the NAC:

(1) NCI, originated in the context of a NAC cooperative activity, shall bear the marking "NATO" followed by the NAC authorised designation of the activity, or by the name(s) of the international organisation(s), or participating nation(s), and the classification level:

Example:

(a) NATO/EAPC RESTRICTED

(b) NATO/SWE CONFIDENTIAL

(c) NATO/ISAF CONFIDENTIAL

(d) NATO/OAE CONFIDENTIAL

(2) The dissemination of information generated within a NATO co-operative activity may be restricted by the originator to some of the non-NATO recipients. In this case, a caveat showing the non-NATO recipients permitted access shall be added below the classification line:

Example:

(a) NATO/PfP RESTRICTED

(b) SWEDEN AND SWITZERLAND ONLY

(3) Information created by a NATO civil or military body that is intended to be further disseminated outside the environment within which it was created shall bear the caveat "Releasable to":

Example:

(a) NATO CONFIDENTIAL
Releasable to AZE

(b) NATO/EAPC RESTRICTED
Releasable to AUSTRALIA

(c) NATO CONFIDENTIAL
Releasable to KFOR

11. **Transmission of Information to be Released.** All NCI released to non-NATO recipients, shall be forwarded via physical or electromagnetic means, in accordance with the requirements of NATO Security Policy and supporting directives.

12. **Records of Information to be Released.** ACO formations shall keep control records of all information classified CONFIDENTIAL and above, which they have released to non-NATO recipients and shall, at least every six months (or as directed by the appropriate Security Authority), report through the chain of command, details of the reference number, title and release date to the NATO Central Registry, Brussels. The report sent to the NATO Central Registry, identifies the details of the information released since the previous report.

13. **Release of NATO Unclassified Information.** Requests for release of NATO Unclassified information are to be addressed to the originating formation or agency. Where the originating formation or agency is unable to authorise release, the matter should be referred to the Military Committee. Within ACO, any officer of OF-5 rank, or civilian equivalent, is permitted to release NATO Unclassified information originated by ACO. Release of NATO Unclassified documents relating to labour or other disputes before national courts and tribunals against any ACO headquarters or organization shall comply will all applicable requirements for the release of NATO Unclassified Information. Failure to follow this policy shall trigger from the ACO headquarters or organization in court a request, through SHAPE, to the national authorities in order to withdraw the NATO secuirity clearances of the individuals releasing NATO Unclassified documents.

ANNEX O TO
AD 070-001
DATED 22 DEC 21

MINIMUM STANDARDS FOR HANDLING AND PROTECTION OF NATO CLASSIFIED INFORMATION UP TO NATO SECRET TO BE MET BY NON-NATO RECIPIENTS

1. **General.** All NCI, which is released to a Non-NATO recipient, is for official use only. It will, therefore, only be disseminated to bodies and individuals with a need-to-know. The minimum standards provided in this document will apply to all NCI released to non-NATO recipients and will also be applied to all classified information exchanged within the context of co-operative activities approved by the NAC.

2. **Personal Security Clearance and Authorisation for Access.** Before a person is granted access to information classified CONFIDENTIAL or SECRET, they shall be subject to a security clearance procedure designed to determine whether they are a loyal and trustworthy individual. When the result of such a procedure is positive, a Security Clearance Certificate will be issued for the individual by their National Security Authority.

3. Before a person is authorised access to classified information, they shall be briefed on the security regulations relevant to the classification of the information released and the legal and disciplinary consequences of breaches of these regulations.

4. When a person who has been security cleared is designated as a representative of their organisation to a meeting in which classified information is involved, or the venue for the meeting is within a secure area, the relevant National Security Authority, when requested, will send a Personnel Security Clearance (PSC) Confirmation to the organisation convening the meeting. The requirements for escorting personnel who do not hold a NATO PSC remain valid if the meeting takes place in a NATO Class I or Class II Security Area.

5. **Registries and Control of Classified Access**. A Registry system shall be established by the recipient for the receipt, dispatch, control and storage of classified information. Sub-registries may be established as necessary. The registry (or sub-registry) will be responsible for:

a. The recording of the receipt and dispatch of all NCI.

b. The distribution and control of classified information within the nation/organisation served.

c. The storage of the classified information.

d. The final disposal of the classified information including the maintenance of:

(1) Destruction certificates for all information classified SECRET.

(2) Log books or document registers for information classified RESTRICTED or CONFIDENTIAL.

REQUIREMENTS FOR THE HANDLING, STORAGE AND TRANSMISSION OF NCI

6. **NATO RESTRICTED.** Information shall be handled, displayed, processed and stored in a manner that deters unauthorised access; for example, in a locked desk, cabinet

or room to which access is controlled. Documents may be sent through postal channels by such means as are authorised by the appropriate NSA. Cryptographic systems approved by a NATO member nation or by the NAMILCOM shall be used for the encryption of NATO RESTRICTED information transmitted by electromagnetic means. In exceptional circumstances, when speed is of paramount importance and means of encryption are not available, information classified NATO RESTRICTED may be transmitted electromagnetically in clear text over public systems. Reproductions and translations of documents classified NATO RESTRICTED may be produced by the addressee under strict observation of the need-to-know principle.

7. **NATO CONFIDENTIAL.** Information shall be handled, displayed, processed and stored in areas to which access is strictly controlled. Access shall be restricted to designated individuals who have been appropriately cleared and have an established need-to-know for official purposes. Information shall be stored in security containers with nationally approved locks, the keys or combinations which shall be held by designated security personnel. Transmission of documents must be by official courier or diplomatic bag. Cryptographic systems approved by a NATO member nation or by the NAMILCOM shall be used for the encryption of NATO CONFIDENTIAL information transmitted by electromagnetic means. Reproductions and translations of documents classified NATO CONFIDENTIAL may be produced by the addressee under strict observation of the need-to-know principle.

8. **NATO SECRET.** Information shall be handled, displayed, processed and stored in areas to which access is strictly controlled. Access shall be limited to designated appropriately cleared individuals with an established need-to-know for official purposes. NATO SECRET information shall be stored in security containers with nationally approved locks, the keys or combinations which shall be held only by designated security cleared personnel needing access to the stored information to fulfil their official duties. Transmission of documents must be made by official courier or diplomatic bag.

9. Only cryptographic systems specifically authorised by the NAMILCOM shall be used for the encryption of information, regardless of the means transmitted (e.g. electromagnetic), which is classified NATO SECRET. Reproductions and translations of documents classified NATO SECRET may be produced by the addressee under strict observation of the need-to-know principle. Copies of documents classified NATO SECRET must be marked with identifying reproduction copy numbers. The number of reproductions and/or translations of NATO SECRET documents and their copy numbers must be recorded by the registry (or sub-registry).

10. **Communications and Information Systems**. Non-NATO communication and information systems used for the processing/storage/transmission of NCI shall meet the standards required by NATO Security Policy and supporting directives.

11. A balanced set of security measures (physical, personnel, procedural, computer and communication) shall be identified and implemented to create a secure environment in which CIS operates.

12. Computer security measures (hardware and software security features) shall be required to implement the need-to-know principle, and to prevent or detect the unauthorised disclosure of information. The extent to which computer security measures are to be relied upon shall be determined during the process of establishing the security requirement and the ability of such measures to provide the required level of security will

be verified.

13. The integration of an ADP system and a communications system shall also require that the communications security aspects be assessed as part of the overall security.

14. **Breaches or Compromise of Security.** Whenever a breach/compromise of security affecting classified information is discovered, the following action is to be taken in conjunction with Part VI, Chapter 1:

a. A report giving details of the breach/compromise must be sent immediately to the NOS via the chain of command and to the Release Authority who will inform the originator(s) as required.

b. An investigation into the circumstances of the breach/compromise must be carried out immediately. Once completed, a full report will be submitted to the NOS via the chain of command. At the conclusion of the investigation, remedial or corrective action, where appropriate, shall be taken and the NOS notified. In all cases the originator shall be informed.

c. Investigation reports shall contain the following information:

(1) A description of the information involved, including its classification and marking, reference number(s) and copy number(s); the date of the classified information, originator, subject and scope.

(2) A description of the circumstances of the compromise, including the date, the period during which the information was exposed to compromise and, if known the number and/or category of unauthorised individuals who had or could have had access to the classified information.

(3) The time and date that the originator of the classified information was informed of the breach/compromise.

15. **Inspections.** A non-NATO recipient participating in a NAC-approved activity shall facilitate periodic inspections by the NOS to ensure that the security arrangements for the protection of released information meet the minimum standards established by the NOS.

ANNEX P TO
AD 070-001
DATED 22 DEC 21

SECURITY ARRANGEMENTS FOR THE RELEASE OF NATO CLASSIFIED INFORMATION TO THE EUROPEAN UNION

1. The release and exchange of information classified NATO RESTRICTED and above between NATO and the European Union (EU) is regulated by the Security Agreement between the two parties. This Annex set out the policy, procedures and regulations required for the release of NCI to the EU.

2. **Eligibility for Receipt by EU of NATO Classified Information.** NATO members in the EU are eligible to receive information classified up to and including COSMIC TOP SECRET (CTS), via the EU. Non-NATO members in EU must have completed all security formalities and signed a security agreement with EU to be eligible to receive information classified up to and including NATO SECRET.

3. **Release Authority.** The North Atlantic Council (NAC) is the ultimate authority for the release of NCI to the EU. Except for information classified up to and including COSMIC TOP SECRET, which has been originated by the NATO Military Committee (NAMILCOM) (see (b) below), the release of information classified COSMIC TOP SECRET will always rest with the NAC. A committee may agree on the advantage of disseminating such information to the EU, however, it must obtain NAC approval for its release.

4. The NAC has delegated release authority to the following bodies:

a. The relevant committee for information classified up to and including NATO CONFIDENTIAL.

b. The NAMILCOM for information classified up to and including COSMIC TOP SECRET, which has been originated by the NAMILCOM, and bodies subordinate to it.

c. The Board of Directors of a NATO Production and Logistics Organization (NPLO), for information classified up to and including NATO SECRET originated by and belonging to one or more of the states participating in the NPLO.

5. Authority for release will only be delegated to a committee on which the originator(s) is/are represented. If the originator(s) cannot be established, the relevant committee will assume the responsibility of the originator(s).

6. **Procedures to be Followed for the Release of NATO Classified Information to EU Requests for Release.** Requests from EU for release of NCI (stating their requirement and giving details of intended recipients) will be sent to the relevant addressee as follows:

a. The Executive Secretary, NATO International Staff, for NCI issued by the NAC and bodies subordinate to it.

b. The Director, International Military Staff, for NCI issued by the NAMILCOM and bodies subordinate to it.

c. The Head of a NPLO for classified information originated by and belonging to one or more of the states participating in that NPLO.

7. **Actions upon Receipt of a Release Request.** The addressee will task relevant NATO staffs to prepare required documents for the appropriate committee (or, in the case of an NPLO, for the Board of Directors or any other body designated to authorise release) for a decision on release. These documents will contain the following information:

a. The identity of state(s) eligible for receipt under the terms of the request.

b. In the case of release requests to non-NATO member states of the EU, written confirmation that the EU has completed security formalities and has signed a Security Agreement with those non-NATO member states; this will be provided through the NOS.

c. Identification of the document(s) containing the NCI (reference number, date and NATO security classification).

d. A description of the NCI, which could be released (the whole document(s), part of the document(s) or excerpts from the document(s)).

8. **Requests for Generic Release.** Requests for generic release will also include, as appropriate, details of specific subject areas, defined series of documents, anticipated future documents or series of documents and anticipated requirements for internal release, etc., stating maximum classification. Upon approval, the appropriate committee (or Board of Directors) will state any other limitations regarding future release.

9. **Processing Release Requests**. Requests will be sent to the appropriate committee (or Board of Directors) for a decision, which will entail obtaining the approval of the originator(s). National members of the relevant committee are responsible for obtaining any clearance, which may be required from their national authorities. The Board of Directors of an NPLO, having agreed on the release of classified information originated by and belonging to one or more of the states participating in the NPLO, will then seek the approval of the national security authorities of the nations participating in the NPLO for its dissemination.

10. In cases where the NCI requested for release has been issued by two or more bodies (e.g. a military document prepared by NAMILCOM and approved by Defence Planning Committee (DPC) and issued under the latter's reference), it is the responsibility of the initial addressee to coordinate the response to the request.

11. **Classification Markings.** Classified information originating from NATO, which is released to the EU, will retain its NATO ownership label and security classification. The NATO-EU security agreement (SG(2003)0186) covers the rules regarding the exchange of classified information between NATO and the EU (RESTRICTED, CONFIDENTIAL and SECRET). Unless otherwise stated by the originator, as a principle, documents should only be shared between the staffs of the two organisations and shall not be disseminated further. Therefore, for political reasons, the security marking 'NATO (CLASSIFICATION) RELEASABLE TO THE EU' should be avoided.

12. ACO staffs should instead use markings such as 'NATO (CLASSIFICATION) RELEASABLE TO THE EEAS and/or THE EUROPEAN COMMISSION and/or THE

GENERAL SECRETARIAT OF THE COUNCIL OF THE EUROPEAN UNION'.

13. The only EU Institutions that can receive NCI are:

a. The General Secretariat of the Council of the European Union.

b. The European Commission.

c. The European External Action Service (EEAS).

Note: Other EU Institutions, such as the European Parliament, or Agencies, such as the European Defence Agency or FRONTEX are not covered by the security agreement between NATO and the EU and the exchange of classified information with them is not permitted. The only exception to this rule is if there are ad-hoc agreements between a NATO Military body or Agency and an EU Agency, for instance, between MARCOM and FRONTEX regarding the exchange of information classified as RESTRICTED in the context of Aegean Sea activity.

14. In addition, the cover or first page of any document released will be marked with the name of the committee (or Board of Directors), which has authorised the release, the date the release decision was taken and any related terms.

15. **Records.** NATO bodies shall maintain complete, separate records of all NCI, which they have released to the EU and will send details of the reference number; title and release date to the NATO Central Registry, Brussels.

16. **Security Regulations for the Handling of NCI Released to EU.** All NCI, which is released to the EU, is for official use only. It shall, therefore, only be disseminated to individuals in the EU with a need-to-know and in accordance with stipulated release caveats. Within the EU, NCI shall be handled in accordance with EU security regulations, which are based on NATO regulations.

17. **Personnel Security Clearance and Authorisation for Access.** All individuals who have a need-to-know and require access to information classified NATO CONFIDENTIAL and above must have a valid EU security clearance granted by their National Security Authority.

18. Before being given access to NCI, the individual must be briefed on the protective security regulations relevant to the classification of the NATO information released, their liability to disciplinary action and that such action will not prejudice legal action.

19. **Classification System.** Classification markings will be used to indicate the sensitivity of the NCI and thus the security procedures and regulations, which shall apply for its protection. The classifications are RESTRICTED, CONFIDENTIAL, SECRET and COSMIC TOP SECRET. These classifications correspond to the EU classifications of "RESTRICTED", "CONFIDENTIAL", "SECRET" and "FOCAL TOP SECRET".

20. **Registries and the Control of Classified Information.** A registry system will be established by the EU for the receipt, dispatch, control and storage of NCI. Sub-registries may be established as necessary. The registry (or sub-registries) will be responsible for:

a. Recording of receipt and dispatch of all NCI.

b. The distribution and control of NCI within EU.

c. The storage of NCI.

d. The final disposal of NCI including the maintenance of destruction certificates for all NCI, logbooks or document registers for information classified NATO RESTRICTED or NATO CONFIDENTIAL.

21. **Electrical Transmission.** The electrical transmission of classified information between NATO and EU shall be in accordance with agreed NATO/EU mechanisms/procedures, which assure its protection.

22. **Breaches or Compromises of Security.** Whenever a breach/compromise of security affecting NCI is discovered or suspected, the following actions shall be carried out, in conjunction with Part VI, Chapter 1:

a. A report giving details of the breach/compromise will immediately be sent to the NOS and to the NATO Release Authority who will inform the originator(s) as required.

b. An investigation into the circumstances of the breach/compromise must be made. When completed, a full report must be submitted to the NOS. At the conclusion of the investigation, remedial or corrective action, where appropriate, must be taken.

23. **Reports.** As long as the EU holds NCI, it will submit an annual report, to reach the NOS by the 31st January every year, to confirm the above security regulations are being implemented.

24. **Inspections.** The NOS is responsible, on behalf of NATO, for security arrangements for the protection of classified information and material exchanged between NATO and the EU. It shall therefore carry out regular inspections in the EU of the security measures in force to protect NCI released to the EU.

25. **Requests from NATO for the Release of EU Classified Information.** Following is an example of a request form, which is to be completed and sent to the Secretary General, EU by agreed channels.

AD 070-001

	NATO RESTRICTED
	NATO CONFIDENTIAL
	NATO SECRET
	COSMIC TOP SECRET

NORTH ATLANTIC TREATY ORGANISATION

FROM: (DIVISION/OFFICE)

REQUEST FOR RELEASE OF EU CLASSIFIED INFORMATION

TO : EU (COUNCIL OR COMMISSION, AS APPROPRIATE) INFO. : REFS. :	FILE : NO :
1. IDENTIFICATION OF DOCUMENT(S) (WHERE KNOWN)	
2. RATIONALE FOR THE REQUEST	
3. INTENDED RECIPIENTS IN NATO	
4. (Describe here if the whole document is needed or which part or extract is requested)	

Date: Signature:

ANNEX Q TO
AD 070-001
DATED 22 DEC 21

Date: (DD/MM/YYYY) __/__/____

Optional (Reference Number): ……

REQUEST FOR PERSONNEL SECURITY CLEARANCE CONFIRMATION

1. **Please confirm whether the individual listed below has a Personnel Security Clearance (PSC) to the depicted level.**

Surname:
.....
Forename(s) (as shown on Passport/ID):
.....
Date of Birth (DD/MM/YYYY): __/__/____

Place of Birth:
.....
Nationality:
.....
Passport/ID Number (Optional)
.....
Issued by: .....
Date of issue: (DD/MM/YYYY) __/__/____

2. **PSC required:**

Tick as appropriate, one or more of the following:

[ ] COSMIC TOP SECRET……[30]
[ ] NATO SECRET……..[7]
[ ] NATO CONFIDENTIAL……[7]

3. **Reason for request[31]:**
.....
.....
.....
.....

4. **Requesting Organisation:**
.....
Name of the Security Officer: .....
Phone Number: .....
Email: .....

[30] Add Special Category Designator, where applicable (e.g. ATOMAL, BOHEMIA, CRYPTO)
[31] The activity requiring PSC, its timeframe/duration, any other relevant information
(*) The marking is not part of the template.

ANNEX R TO
AD 070-001
DATED 22 DEC 21

Optional (Reference Number): ……

PERSONNEL SECURITY CLEARANCE CONFIRMATION

1. **Confirmation is hereby given that:**

Surname:
.....
Forename(s) (as shown on Passport/ID):
.....
Date of Birth (DD/MM/YYYY): __/__/____

Place of Birth: .....
Nationality: .....

has been granted a Personnel Security Clearance by the Government of:

.....
in accordance with current NATO regulations, including the Security Annex to C-M(64)39 in the case of ATOMAL information, and is therefore declared suitable to be entrusted with information classified up to and including the level of[32]: .....
Remarks: .....
.....

2. **The validity of this confirmation will expire no later than** (DD/MM/YYYY): __/__/____

3. **Confirming Authority (NSA/DSA/other competent security authority):**

Name: .....
.....
.....
Phone Number: .... ……
Email: .....

Date: (DD/MM/YYY) __/__/____ Signature/Stamp (if applicable)[33] .....

[32] Insert, as appropriate, one or more of the following:
COSMIC TOP SECRET
NATO SECRET
NATO CONFIDENTIAL
Add Special Category Designator, where applicable (e.g. ATOMAL, BOHEMIA, CRYPTO)
[33] Supporting document on national PSC procedures and requirements (AC/35-D/1043) identifies Nations' applicability regarding Signature or Stamp.
(*) The marking is not part of the template.

ANNEX S TO
AD 070-001
DATED 22 DEC 21

NATO INTERNATIONAL VISIT CONTROL PROCEDURES (IVCP)

1. Introduction

a. When NATO international visits involve access to NCI or where unescorted access to Class I/II Security Areas within an ACO component compound is necessary, a visit request will be submitted by the visitor through their Security Officer, to the ACO Project Office, or the subordinated facility to be visited. These visit requests are formalised in the standard Request for Visit (RFV) procedure; however specific rules apply for NATO UNCLASSIFIED (NU) or NATO RESTRICTED (NR) visits.

b. While in principle the requirement for applying the RFV procedure starts when the information concerned is classified NATO CONFIDENTIAL (NC), as well as unescorted access to Class I/II Security Areas, Annex LL identifies nations that require by their laws and regulations an RFV submission for NU or NR visits to their country.

c. Visits involving NU or NR information will be arranged directly between the Security Officer responsible for the visitor and the SO (e.g. APO Security Manager) of the facility/compound to be visited without formal requirements. The SO of the facility to be visited shall submit a visit request to its NSA/DSA or APO as identified in Annex LL on behalf of the visitor. However, visitors are not required to hold a PSC.

d. Where international visits involve access by the visitor to information classified NC or above and/or unescorted access to Class I/II Security Areas, such visits shall be subject to a formal RFV and approval by the NSA/DSA of the facility to be visited, or APO when ACO component is to be visited, following the procedures outlined in this Annex.

2. Scope

a. **General.** The attached standard procedures have been approved for visits by personnel to facilities or ACO component compounds located within another country (e.g. country of operation). They may also be applied to visits within a country of stationing. NATO Member Nations have also agreed to include the procedures in their national regulations that govern international visits. Notwithstanding the agreed procedures, NSAs/DSAs may, for national security reasons, refuse a RFV for a visit to one of its facilities.

b. **Special Arrangements for Specific Programmes/Projects/ Constructions.** While the NATO IVCPs will normally be those defined in this Annex, in the case of a specific programme/project/construction, when all NSAs/DSAs involved, in co-ordination with the responsible APO, determine that these general procedures would not be the best suitable for their specific requirements, they are authorised to establish other procedures, which will be set out in a Project Security Instruction (PSI) that provides a level of protection no less stringent than the principles set out in this Annex:

(1) Accordingly, where permitted by national rules and regulations, visits involving access to information classified up to and including NATO SECRET (NS) may be arranged by exception, directly between the Facility Security Officer (FSO) of the sending and receiving facility, acting on behalf of the NSAs/DSAs involved and APO, provided that such an arrangement is approved by the relevant national authorities and ACO component Security Authority.

(2) International Visits to Non-NATO Nations (NNNs) and International Organisations (IOs) concerning contracts/sub-contracts involving NCI have to adhere to the respective provisions of the relevant Security Agreement or Arrangement in place.

c. **Personnel on Loan within a NATO Programme/Project/Construction.** When an individual (not Contractor) who has been security cleared is to be loaned within a NATO programme/project/construction from one Contractor's facility to another one located in another NATO country, or to a ACO component, the individual may be assigned, or have access to NCI at the facility the individual is to be loaned on the basis of a RFV, or Confirmation of PSC, as appropriate. The RFV or PSC Confirmation shall be provided by the parent NSA/DSA to the APO of the ACO component compound the individual is to be loaned.

3. **Types of Visits and Procedures.** There are four types of international visit requests. They are as follows:

a. One-time.

b. Recurring.

c. Emergency.

d. Amendment.

4. **One-Time Visit**

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 PSC of the visitor(s).

b. 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.

5. **Recurring Visit.** A recurring visit is for intermittent visits over a specified period of time to a specific site or sites and for a specific purpose. A recurring visit normally covers the duration of a government approved programme, project, construction or contract that requires participating personnel to make intermittent (recurring) visits to military, government, ACO component or industrial facilities of another country participating in the programme. Visits covering a period of more than one year may be subject to annual review, as agreed by the participating countries NSA/DSA and an APO. The duration of the visit will never be longer than the validity of the PSC of the visitor(s).

6. **Lead Times for One-Time and Recurring Visits.** The lead time to process one-time and recurring visits is depicted in Annex LL, which identifies the number of working days to the starting date of the one-time, or the starting date of the first of the recurring visit that the request should be provided to the receiving NSA/DSA or APO.

7. **Emergency Visit**

a. 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 in Annex LL cannot be met.

b. Such unplanned or emergency visits should be arranged only in exceptional circumstances. To qualify as an emergency visit at least one of the following conditions must be met:

(1) The proposed visit is related to an official military, government, APO request for proposal/request for tender offer (e.g. submission of, or amendment to, a bid or proposal; attendance at pre-contract negotiations or bidder's conference).

(2) The visit is to be made in response to the invitation of a host government, military, ACO component official or host contract official and is in connection with an official military, government, ACO-led programme/project/construction or contract.

(3) A programme/project/construction, contract opportunity or otherwise significant financial interest will be placed in jeopardy if the visit request is not approved.

(4) Operations and/or personnel are placed in direct jeopardy if the visit is not approved.

c. Emergency visit requests shall be critically reviewed, fully justified and documented by the HQ Security Officer of the requesting ACO component compound or FSO of industrial facility. Therefore, the requestor must complete the remarks portion in item 15 of the RFV Form to fully explain the reasons behind the emergency RFV.

d. When the Security Officer is satisfied that the conditions cited in paragraph 7(b) of this document have been met, the Security Officer will contact an APOSM at the ACO component compound to be visited, to obtain tentative agreement for the proposed visit. If tentative agreement is provided to proceed with the visit request, the APOSM of the ACO component compound to be visited shall then immediately notify its NSA/DSA that an emergency visit request will be submitted by the government agency, organisation, or industrial facility requiring to make the visit (requesting facility) and explain the reason for the emergency. Furthermore, the APOSM shall then follow regular RFV procedures and send the emergency RFV to their NSA/DSA.

e. As there are no lead times for emergency RFV procedures, it is assumed that mutual understanding between the involved parties about the importance of the emergency RFV will result in adequate processing terms.

8. **Amendment**

a. 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.

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

(1) Change of dates of visit.

(2) Addition and/or deletion of visitors.

(3) Change of location.

c. 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 by the receiving NSA/DSA or APO.

d. Changes to the dates of a visit, the addition or deletion of visitors or a change of location to be visited should be reported immediately to the receiving NSA/DSA or APO via the standard procedure. Amendments will be accepted by the receiving NSA/DSA or APO up to the number of working days (assuming 5 working days in one calendar week), prior to the approved or pending visit. The lead time to process amendments is depicted in Annex LL.

9. **Use of the Standard Request for Visit Form**

a. For all types of visit, the standard RFV Form (Tab 2 to Appendix 1 to this Annex) should be used.

b. 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. It is therefore essential that the detailed instructions for completion of a RFV Form described at Tab 1 to Appendix 1 to this Annex be used to fill in each data element. To fulfil this requirement it is advised that Appendix 1 with its two Tabs be used as a hand-out to the visitor through the Security Officer of the agency, organisation or facility or an APOSM. Furthermore, it is advisable to translate those instructions for the use and completion of the RFV Form in the language of the user.

c. The completed RFV is normally an unclassified document.

d. Completion of the RFV Form should be in one of the official NATO languages.

APPENDIX:

1. Standard Form for Request for Visit.

APPENDIX 1 TO
ANNEX S TO
AD 070-001
DATED 22 DEC 21

STANDARD FORM FOR REQUEST FOR VIST

1. The attached guidance contains the instructions for the use and completion of a Request for Visit (RFV) Form when a visit authorisation is required by the receiving organisations or governments. This form standardises the elements required for a RFV and places them in a logical order. The RFV Form can be used for manual as well as automated processing; however, the use of an electronic form and the transmission via e-mail are strongly encouraged.

2. It is advisable to use this Appendix and its two Tabs as a hand-out to the visitor. The general principle of this RFV is that only one format will be used when a visit request is necessary.

3. The following Tabs are contained in this Appendix:

TABS:

1. Instructions for Use and Completion of a Request for Visit.
2. Request for Visit Form (and Annexes thereto).

TAB 1 TO
APPENDIX 1 TO
ANNEX S TO
AD 070-001
DATED 22 DEC 21

INSTRUCTIONS FOR USE AND COMPLETION OF A REQUEST FOR VISIT

1. **General Instructions**

a. The Request for Visit (RFV) shall be completed without mis-statement or omission. Failure to provide all requested information will delay the processing and possibly lead to the denial of the request.

b. This RFV should be typed. Electronic processing and transmitting of the RFV is encouraged. The completed RFV should normally be an unclassified document. The RFV Form should be written in English.

c. The RFV shall be in the possession of the receiving host NSA/DSA or APO in accordance with the RFV lead times detailed in Annex LL.

d. The completed RFV shall be submitted to the Security Officer of the requesting agency, organisation or facility or APOSM. 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**

a. 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, ACO component, 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 Class I/II Security Areas 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 ORGANISATION OR INDUSTRIAL FACILITY 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 (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: (1) 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...). (2) 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. (3) 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 OR UNESCORTED ACCESS TO SECURITY AREAS	Select the appropriate checkbox for the anticipated highest level of classified information or unescorted access to Class I/II 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 PSC 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:* *(1) Insert name, address, telephone number, and e-mail address.* *(2) Date and signature.* *(3) 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.* *(1) Insert name, address, telephone number, and e-mail address.* *(2) Date and signature.*
16 REMARKS	(1) 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. (2) This item can be used for certain administrative requirements (e.g. proposed itinerary, request for hotel, and/or transportation, etc.). (3) This space is also available for the receiving NSA/DSA for processing (e.g. "no security objections", etc.). (4) In case a special briefing is required, the type of briefing and the date that the briefing was given should be stated.

ANNEX 1 - GOVERNMENT AGENCY, ORGANISATION OR INDUSTRIAL FACILITY 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: (1) For visits to the United States, one RFV Form with Annexes for each agency/organisation/facility to be visited should be filled in. (2) 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 – PATICULARS OF VISITOR	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 dd/mm/yyyy. POB: Place of birth (city-province/state-country). Nationality: Insert nationality as per passport. Security clearance level: Actual PSC status (e.g. TS, S, C). Indicate NATO PSC (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.

TAB 2 TO
APPENDIX 1 TO
ANNEX S TO
AD 070-001
DATED 22 DEC 21

REQUEST FOR VISIT[34]

TO: _____

(Country/NATO body)

1. Type of Visit Request	**2. Type of Information/ or Site Access**	**3. Summary**
☐ One-time ☐ Recurring ☐ Emergency ☐ Amendment ☐ Dates ☐ Visitors ☐ Agency/Facility For an amendment, insert the NSA/DSA original RFV Reference No.	☐ NATO CONFIDENTIAL or above, and/or ☐ Access to Class I/II Security Areas.	No. of sites: _____ _____ No. of visitors: ___

4. Administrative Data:

Requestor: To:	NSA/DSA RFV Reference No. _____ Date

5. Requesting Government Agency, Organisation or Industrial Facility:

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

Name:
Postal Address:
E-Mail Address:
Fax No:
Telephone No:

6. Government Agency, Organisation or Industrial Facility to be Visited
(Annex 1 to be completed)

[34] All fields must be completed.

7. Date of Visit (dd/mm/yyyy): From _____/_____/_____ To _____/_____/_____

8. Type of Initiative (select one from each column):

☐ Government initiative	☐ Initiated by requesting agency or facility
☐ Commercial initiative	☐ By invitation of the facility to be visited

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- (Annex 2 to be completed)

AD 070-001

13. The Security Officer of the Requesting Government Agency, Organisation or Industrial Facility:

Name:

Telephone No:

E-Mail

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 (e.g. APO):

Name:

Address:

Telephone No:

E-Mail Address:

Signature: Date (dd/mm/yyyy): ____/_____/_____

16. Remarks *(*mandatory justification required in case of an emergency visit):

AD 070-001

ANNEX 1 to RFV Form

Government Agency, Organisation or Industrial Facility 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:
(Continue as required)

AD 070-001

ANNEX 2 to RFV Form

PARTICULARS OF VISITOR(S)
1. ☐ **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: Personnel Security Clearance Level: PP/ID Number: Position: Company/Agency:
2. ☐ **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: Personnel Security Clearance Level: PP/ID Number: Position: Company/Agency:
(Continue as required)

AD 070-001

ANNEX 3 to RFV Form

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

COUNTRY	OFFICE	E-mail
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
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

COUNTRY	OFFICE	E-mail
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
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

ANNEX T TO
AD 070-001
DATED 22 DEC 21

BRIEFING ON PROCEDURES FOR SAFEGUARDING COSMIC TOP SECRET AND ATOMAL INFORMATION

1. Your division chief has authorised you to have access to COSMIC TOP SECRET and ATOMAL (CTS/A) information on a strict need-to-know basis, in the performance of your duties.

2. This means that your name will be placed on the List of personnel authorised access to COSMIC TOP SECRET and ATOMAL (CTS/A Access List (ACO Form 120(A) or ACO Form 120(C)) information of your division.

3. The CTS/A Access List is a list of those individuals possessing the NATO CTS/A clearance who have been indoctrinated regarding the handling of CTS/A information, and who have signed the CTS/A Briefing Certificate (ACO Form 107). The type of access authorised is indicated on the CTS/A Access List.

4. The full details regarding the handling of CTS/A information are set out in the above references. Should you require more guidance on the handling of CTS/A information, you should first consult your HQ COSMIC and ATOMAL Control Officer (CACO) or DSO who will provide the referenced documents for your perusal and give any additional advice required. When originating NATO documents which contain ATOMAL information, you are to refer to C-M(68)41 and to ascertain the correct classification to be applied.

5. ATOMAL information is either “US Atomic information” released under NATO ATOMAL markings which is provided by the Government of the United States of America to other NATO component; or “UK ATOMIC information” which is provided by the Government of the United Kingdom to other NATO components.

6. Documents (less films, slides, etc.) containing United States atomic information communicated under the Agreement bear NATO markings and a security classification equivalent to that assigned by the government of the United States of America, followed by the word ATOMAL. In addition, the following is entered on the document in the language of the document: "This document contains United States atomic information (restricted data or formerly restricted data) made available pursuant to the NATO Agreement for Cooperation Regarding Atomic Information dated 18 June 1964, and will be safeguarded accordingly".

7. Films, slides, etc. will bear the word ATOMAL together with the security classification, e.g. COSMIC TOP SECRET ATOMAL, or NATO SECRET ATOMAL.

8. The CACO must be engaged for accountability and control of all documents containing CTS/A information, including notes taken during meetings. When it is necessary to translate, reproduce, extract from, or generate CTS/A documents, the CACO shall be contacted for specific security guidance.

9. If you are required to obtain a CTS/A document from the division CTS/A Control Point (CP) or from the HQs’ CTS/A Sub-Registry, you must sign a receipt, which transfers the responsibility for the document to you. This implies that:

a. The CTS/A document is used only in HQ Security Areas in which every possible precaution has been taken to prevent unauthorised or inadvertent disclosure of the information to unauthorised persons.

b. The CTS/A document must never be left unattended in circumstances where persons who are not authorised access to CTS/A information might obtain access to the document.

c. The CTS/A document will not be carried about unless it is covered in such a way as to conceal its contents.

10. If you need CTS/A data during meetings or conferences to be held outside your headquarters, it is necessary to arrange to have the data sent in advance by an authorised courier, via the ACO CTS/A Registry System, to a NATO component which has been certified as having the means to provide adequate security protection to CTS/A information.

11. A Disclosure Control Record (ACO Form 78) will be attached to all CTS/A documents/messages. Such a record will also be attached to all NATO SECRET ATOMAL and NATO CONFIDENTIAL ATOMAL documents on which SPECIAL LIMITATIONS have been placed. All persons who have had access to, and knowledge of the contents of, such documents shall sign the Disclosure Control Record form on each occasion that such access is made.

12. CTS/A information shall not be mentioned in the presence of a person who is not CTS/A cleared, nor shall such information be discussed on a telephone.

13. Compromise of CTS/A can result just as easily from negligence, carelessness or indiscretion as from espionage.

14. It is imperative for you to inform your Division Security Officer (DSO) immediately of any possibility of a compromise of CTS/A information, to minimise any possible damage to NATO interests.

15. Accordingly, you are requested to comply with the above requirements by signing, in the presence of a witness, the attached ACO Form 107 and returning it as soon as possible to the DSO. Annually, hereafter, while you retain your authorisation for access to CTS/A information, this certificate will be returned to you for reaffirmation that you understand the procedures for handling CTS/A information.

16. Please retain this briefing letter for your use and as a reference guide.

ANNEX U TO
AD 070-001
DATED 22 DEC 21

Optional (Reference Number): ……..

PERSONEL SECURITY CLEARANCE CONFIRMATION
(for non-NATO citizens)

1. **Confirmation is hereby given that:**

Surname:
.....

Forename(s) (as shown on Passport/ID):
.....

Date of Birth (DD/MM/YYYY): __/__/____

Place of Birth: .....

Nationality: .....

has been granted a Personnel Security Clearance by:
.....

in compliance with a security investigation process no less stringent than that of NATO, has been briefed on the security regulations for the protection of NATO Classified Information and the legal and disciplinary consequences of infraction/breaches of those regulations, and is, therefore, declared suitable, in accordance with the provisions of the Security Agreement between NATO and [*Non-NATO Entity*], to be entrusted with information classified up to and including:

NATO SECRET/CONFIDENTIAL[35]

Remarks: .....
.....

2. **The validity of this confirmation will expire no later than** (DD/MM/YYYY): __/__/____

3. **Confirming Authority / National Security Authority:**

Name: .....
.....
.....
Phone Number: .....
Email: .....

Date: (DD/MM/YYYY) __/__/____ Signature/Stamp: .....

[35] Delete as appropriate.
(*) The marking is not part of the template.

ANNEX V TO
AD 070-001
DATED 22 DEC 21

SECURITY AWARENESS PROGRAMME CONTENT

1. **Security Awareness Programme Content.** A security awareness programme coordinates the objectives and methods of security awareness in order that individuals are informed about the importance of security both at the beginning of their duties and also subject to periodic reminders. As a minimum, the following key topics shall be covered:

a. **Security Organisation.** As a minimum, the content in this domain should include:

(1) Description of the security authorities in the Organisation, their roles and responsibilities;

(2) Description of the points of contact for emergencies and reporting of incidents; and

(3) Confirmation of the support of the senior management for the security framework.

b. **Personnel Security.** As a minimum, the content in this domain should include:

(1) Information about the threats from terrorism, espionage, intelligence services, subversion or sabotage;

(2) Information on the security aspects and conduct to be observed when travelling to countries with special security risks;

(3) The risk arising from conversations, in person or via electronic means, involving classified information with individuals having no need-to-know and/or who lack the appropriate Personnel Security Clearance (PSC), as applicable;

(4) Staff's responsibilities related to continuous affirmation, with their behaviour and actions, of their eligibility for a PSC;

(5) Explanation of the role of managers related to aftercare;

(6) A general reminder of all staff's obligation to meet the security requirements linked to the post they are fulfilling within the Organisation;

(7) Procedures for staff authorised to escort visitors into the working areas, duly described and highlighting the aspects for which staff are responsible; and

(8) Security instructions to be observed by non-staff individuals (e.g. contractors, visitors) during their presence on site. In some cases, this might include a signing of a Non-Disclosure Agreement (NDA), following the provision of a security briefing.

c. **Physical Security.** As a minimum, the content in this domain should

include:

(1) Description of the physical security features that staff might experience accessing and working on site;

(2) Description of procedures or processes that involve staff's knowledge and cooperation for being effective, explained in terms of functionality, focusing on the importance of staff diligence as instrumental in achieving intended security objectives;

(3) Education on the importance and the relevant provisions related to the implementation of a robust access control to sensitive areas and CIS;

(4) Indication of the presence and value of security measures (e.g. biometrics), which might be perceived as more intrusive by some individuals in terms of affecting their personal sphere (e.g. physical contact, privacy);

(5) Description of the signage, warning and alerting systems in use at the Organisation, particularly those dealing with safety and security measures; and

(6) Explanation of the different types of security areas, the way they are determined and how staff should operate CIS and handle information inside these areas.

d. **Security of Information.** As a minimum, the content in this domain should include:

(1) The appropriate classification and markings of information, as required by the Organisation;

(2) How information should be handled within the work environment (e.g. dissemination, reproduction, destruction, downgrading of classification, declassification);

(3) How the information should be handled outside the Organisation (e.g. during physical transfer from one point to another either within or outside of the Organisation's site);

(4) Description of the element in charge of accounting for information and providing the related support and guidance (e.g. Registry);

(5) Possible violation of security of information due to usage of mobile applications and social media; and

(6) Description of instruments and/or restrictions related to information sharing with third parties.

e. **CIS Security.** As a minimum, the content in this domain should include:

(1) Description of the CIS provided by the Organisation and the level of classification that may be handled within;

(2) Indication of the applicable CIS-specific Security Operating

Procedures (SecOPs);

(3) Indication of which privately owned CIS are allowed on site and the local regulations to be followed in this respect;

(4) Illustration of what restrictions are in place for the use of wireless connectivity, mobile networks, tethering, hotspots and other similar technologies;

(5) Description of the Acceptable Use Policy for Internet connectivity provided on site;

(6) Information about specific types of cyber-attacks (e.g. advanced persistent threats) affecting CIS users, at work and at home, perpetrated via social media, emails and other electronic means;

(7) Emphasis of the importance to adopt a CIS Security posture that remains consistent irrespectively of using a CIS at home (i.e. privately owned) or at work (i.e. Organisation owned); and

(8) Explanation on staff's responsibilities in preventing/mitigating technical attacks and their effects (e.g. eavesdropping attacks), identifying the instructions to be followed by the staff while working on premises.

f. **Industrial Security.** As a minimum, the content in this domain should include:

(1) Security requirements for the protection of NCI in contracting;

(2) Description of instruments related to contract-related security provisions (e.g. Contract Security Clause, Security Aspects Letter, Project Security Instructions);

(3) Role of a Facility Security Officer;

(4) Role of the relevant authorities (e.g. Designated Security Authority (DSA), National Security Authority (NSA), Contracting Authority) involved in the security aspects of contracting, as applicable;

(5) Description of the relevant industrial security clearances related to contracts involving NCI at the level NATO CONFIDENTIAL and above (i.e. Facility Security Clearances and Personnel Security Clearances);

(6) Explanation of International Visit Control Procedures (ICVPs); and

(7) Procedures for transmission and transfer of NCI.

g. **Counter-Terrorism.** As a minimum, the content in this domain should include:

(1) General information about the current threat environment;

(2) Explanation of the security alert states and the associated security measures;

(3) Instructions for immediate actions during a bomb or light weapons

attack;

(4) Instructions with respect to the discovery of suspicious packages; and

(5) Procedures to be followed in case of a terrorist attack, including attacks by armed Unmanned Aerial Vehicles (UAVs).

h. **Counter-Espionage.** As a minimum, the content in this domain should include:

(1) General information about the threat landscape;

(2) Description of most common and growing intelligence collection methods and techniques, as wells as the relevant mitigating measures;

(3) Information on most common threats applicable to CIS (e.g. social engineering) with directions on how to prevent and react to such attacks;

(4) Protective measures and precautions to follow in order to minimize the susceptibility to exploitation during travel to countries with particular risk;

(5) The risk to the Organisation stemming from relationships with media, including clarification of the Organisation’s social media use policy; and

(6) Instructions and follow-up procedures in case of a suspected espionage attempt.

ANNEX W TO
AD 070-001
DATED 22 DEC 21

[Insert name of HQ] **– QUARTERLY SECURITY RETURN for** *[Q1 – Q4 +year[36]]*

1. **Staffing**

SECURITY APPOINTMENTS						
Appointment	**Rank, Name, Appointment**		**Letter of Delegation**		**Date of Letter**	
Delegated Authority			**(from COS SHAPE insert Yes or No)**			
Functional Area	**PE**	**Available Security Personnel** *(first name, last name, rank, nationality)*	**Phone Number**	**End of Tour**	**Trained[37]**	**Date of Planned Training**
HQ Security Office						
HQ Security Policy Advisory Staff[38]						
CIS Security Policy Advisory Staff						
Personnel designated to cope with handling and control of COSMIC and ATOMAL material within HQ[39]						

[36] Q1: 01 Jan-31 Mar / Q2: 01 Apr-30 Jun / Q3: 01 Jul-30 Dec / Q4: 01 Oct-31 Dec (i.e. Q1 2021 or Q3 2023)
[37] Yes/No (obligatory training as indicated in job description)
[38] J2X level.
[39] HQ CACO, HQ DCACO, ACO CTS/A Central Registry CCO, ACO CTS/A Central Registry DCCO and Alternates, HQ CTS/A Sub-Registry/Control Point CCO, HQ Sub-Registry DCCO and Alternates.

AD 070-001

2. **Security Incidents / Violations:** Give brief description of the most common security violations observed during reporting period[40]:

SECURITY VIOLATIONS OBSERVED	
TYPE OF VIOLATION	**ACTION TAKEN**

3. **Breaches of Security:** Give details of any breaches of security (NC and above) observed during reporting period:

SUMMARY OF BREACHES OF SECURITY				
Date Reported	**Classification of Material Involved**	**Type of Incident**	**Date of Initial Report**	**Action Taken** *(Give a brief summary of incident, results of investigation, remedial action taken).*

4. **Security Incidents Resulting in Compromise of NATO Classified Information:** Give details of security incidents reported during the period when NATO classified information was compromised.

SUMMARY OF SECURITY INCIDENTS/VIOLATIONS RESULTING WITH COMPROMISE OF NATO CLASSIFIED INFORMATION				
Date Reported	**Classification of Material Involved**	**Type of Incident**	➢ **Intentional** ➢ **Unintentional** ➢ **Not Known**	**Action Taken** *(Give summary of the outcome of the investigation, brief damage assessment and remedial action taken)*

[40] Minor instances of security, not resulting with breaches of security.

5. **Quarterly COSMIC TOP SECRET and ATOMAL Spot Check**[41]

SPOT-CHECKED MATERIAL		
Classification/Category	**Number of Checked Material**	**Log Numbers of Checked Material**
COSMIC TOP SECRET		
ATOMAL		

Comments[42]:

6. **Email Violations:**

EMAIL VIOLATIONS		
Classification	**Number**	**Important details**
NATO CONFIDENTIAL		
NATO SECRET		

Comments[43]:

[41] Results of 25% spot-check of CTS/A holdings done by HQ CACO and provided in Q1, Q2 and Q3.
[42] Confirm check of all receipts and destruction forms generated since the last quarterly spot-check or annual inventory.
[43] Also brief information on NATO Restricted email violations.

AD 070-001

7. ACO CIS Node Security Posture Assessment

No	Question	Scoring(on No)	Value
1.	Is a Business Continuity Plan (BCP) developed and in place?[44]	1	
2.	Is a Disaster Recovery Plan (DRP) developed and in place?	1	
3.	Have those plans been successfully tested and/or executed?	1	
No	**Question**	**Scoring** (on No)	**Value**
4.	Are the GSE and LSE(s) (physical security) compliant with NATO policy?[45]	2	
5.	Is the ESE compliant with NATO policy?	1	
6.	Is the local security documentation up to date (e.g. Sec Ops)?	1	
7.	Are local CIS security processes (e.g. USB management) documented?[46]	1	
8.	Is a local Critical Information List (CIL) developed and maintained?	1	
9.	Is the local Data Loss Prevention tool configured accordingly?[47]	1	
10.	Is the local industrial security element managed (e.g. contractors, supplies, HVAC, etc.)?	1	
11.	Is the local critical infrastructure support identified (e.g. food, water, power, sewage, HVAC, etc.)?	1	
12.	Is the local CIS supporting the critical infrastructure identified?[48]	2	
13.	Is the local critical infrastructure support managed accordingly?	2	
14.	Is a local industrial security policy and support arrangement in place?	1	
15.	Is the local personnel receiving security awareness education or training?	2	
16.	Last ACO inspection result: Marginal	1 (on yes)	
17.	Last ACO inspection result: Unsatisfactory	2 (on yes)	
18.	Last VA result: Marginal	1 (on yes)	
19.	Last VA result: Unsatisfactory	2 (on yes)	
20.	Potential special countermeasures (assessed by SHAPE J2X)	0 to 5	
	Score Summary:	**Overall: 25**	**Actual:**

Note: Mark any question not applicable, or that you are not able to answer, accordingly, as it will be reflected in the ranking.

44 To be reviewed annually, or until a critical change / incident happened.
45 AD 70-1 & ACO Security Accreditation Strategy.
46 For example inside the Sec Ops or a local security supplement.
47 Local CIS Security officer has to verify installation parameters provided by NCIA.
48 CIS required operating services like water treatment facilities, HVAC, power substations, etc.

AD 070-001

Comments:

8. **Security Training:** Give details of any Security / CIS Security training events conducted during reporting period:

SECURITY TRAINING			
Date	**Event**		**Comments**
	Internal	**External**	

Comments[49]:

9. **Identified Trends / Current Security Concerns.** Highlight any emerging trends identified over the reporting period, what remedial action was been taken to mitigate the issue and what future action is planned for the next quarter.

SECURITY ASSESMENT			
Functional Area	**STATUS[50]**		
Personnel Security			
Document Security			
Physical Security			
CIS Security			

Comments:
NAME:
RANK:
APPOINTMENT[51]:

[49] Give information on attendance to NATO Security Course in NATO School, how many seats are available for HQ and how many seats are booked for HQ security personnel.
[50] Mark with X as appropriate (assessment shall be based on security inspection checklist); if a status (trend) has changed, please explain why.
[51] HQ Security Authority.

AD 070-001

GUIDANCE ON CIS SECURITY POSTURE ASSESSMENT

1. **Background**

a. The CIS Security posture assessment is point 6 of the Quarterly Security Return (QSR) and ACO Commands are requested to complete it annually or when the security situation changes.

b. The assessment begins with Phase 1, where an initial set of 20 questions are asked. The questions are intended to cover, in a very high-level manner, the entire spectrum of security criteria that J2X would like to evaluate. Subsequent to the submission of a completed Phase 1, a Phase 2 follow-up questionnaire might be more in-depth by expanding on the original points.

c. The overall outcome is meant to provide J2X with a comprehensive view of the security posture at ACO and subordinate operational commands. This will serve as the basis for 'situational awareness' and will support the potential introduction of security countermeasures to decrease the overall threat level.

2. **Objective**

a. The main goal of the questionnaire is to assess a wide spectrum of security-related aspects of day-to-day operations. From physical security to authentication, the defences are collectively intended to provide a defence in-depth capability against common and foreseeable, but also unforeseeable, threats to NATO computer systems and computer networks.

a. The questions are designed to be closed and value-based. The overall score will determine the severity of the risk posed to each command by the various existing and predictable security threats.

b. Results of the evaluation shall be reported to HQ J2X in the first QSR of the year, and fed up the chain of command.

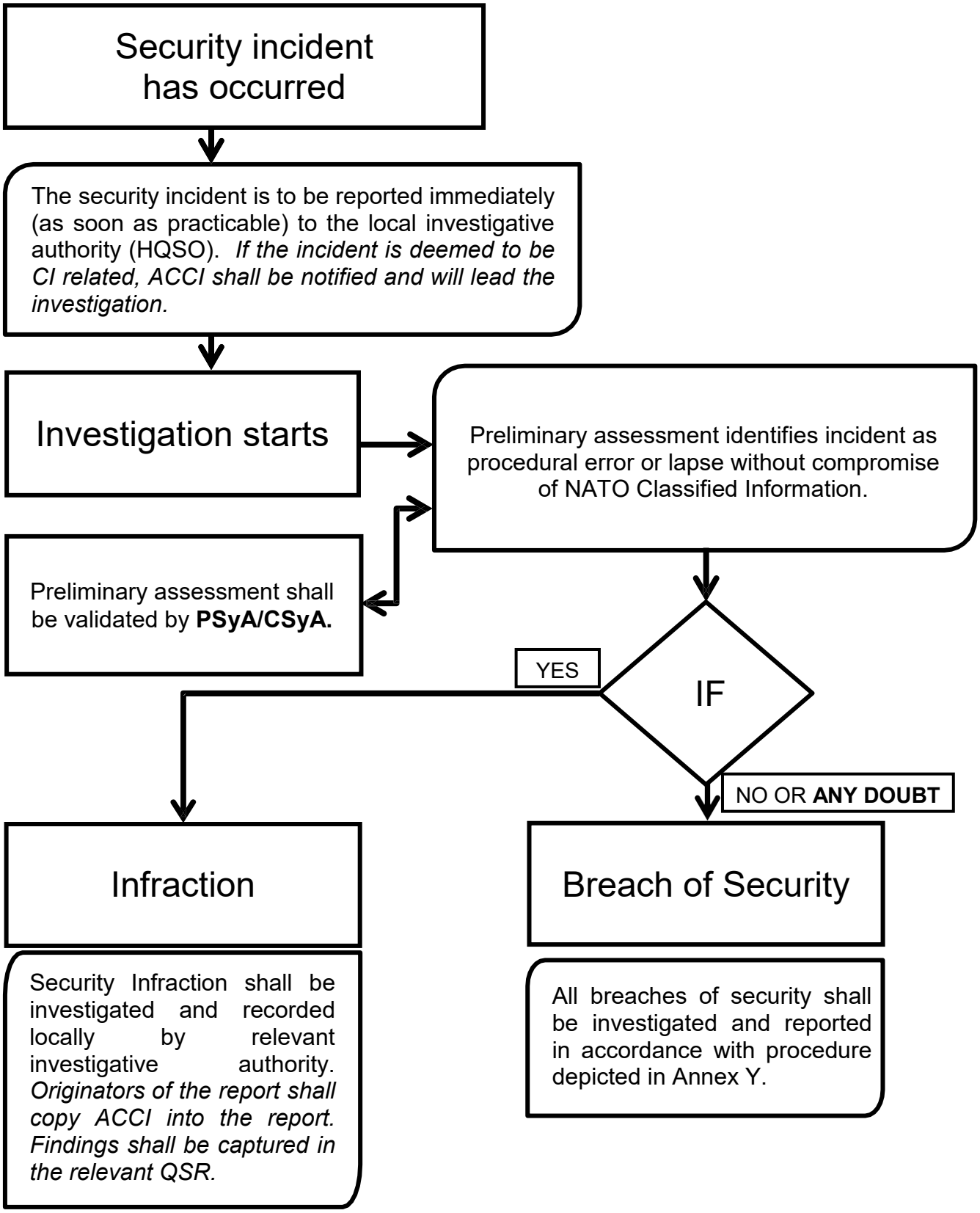
c. The ultimate authority over the assessments is exercised by SHAPE J2X CIS Security.

b. The expected outcome and ranking of the security posture is as follows:

24 – 25	Critical
21 – 23	Severe
16 – 20	Moderate
10 – 15	Good
0 – 9	Excellent

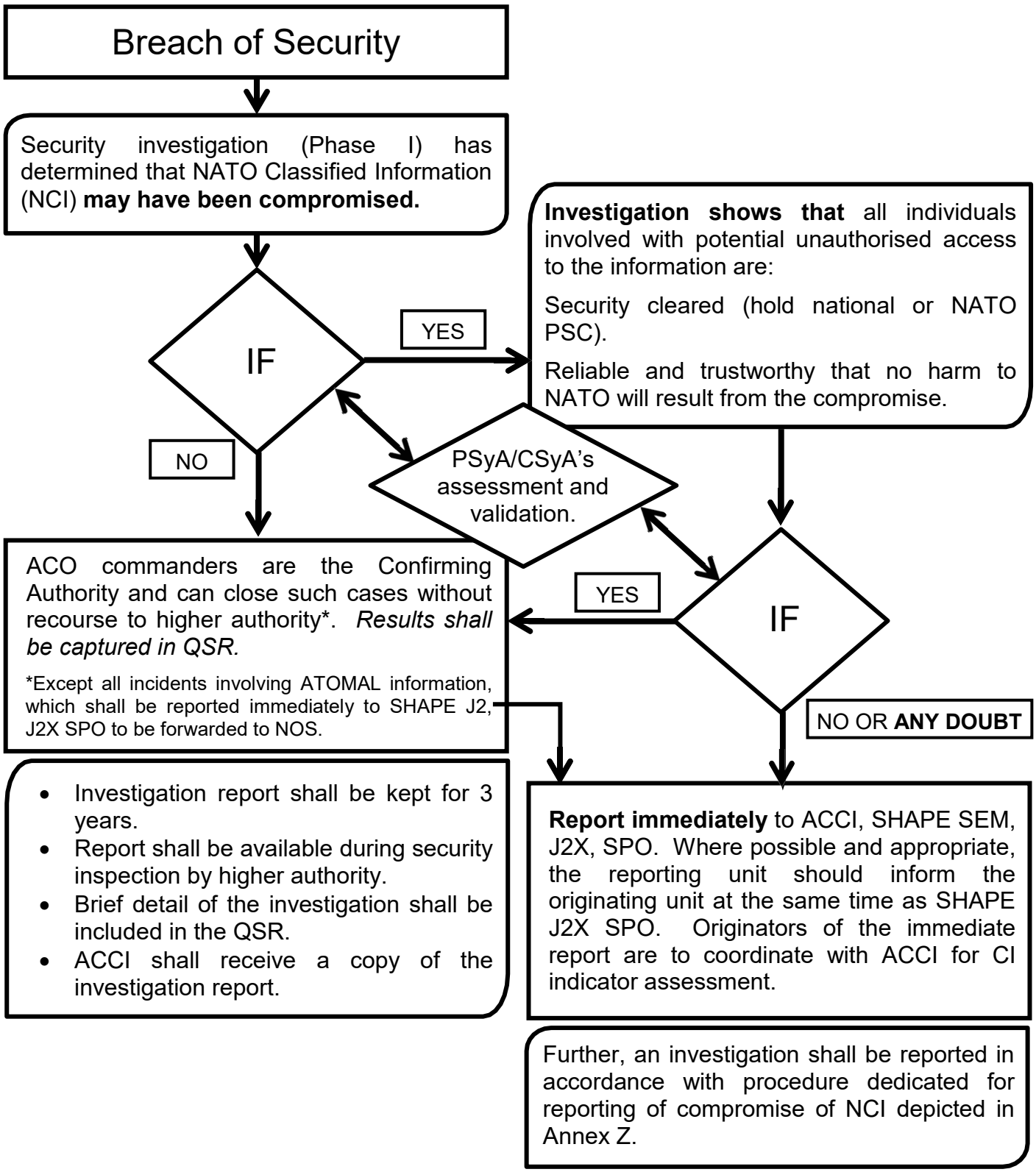
ANNEX X TO
AD 070-001
DATED 22 DEC 21

SECURITY PROCEDURES FOR PHASE I – EVALUATION OF SECURITY INCIDENT



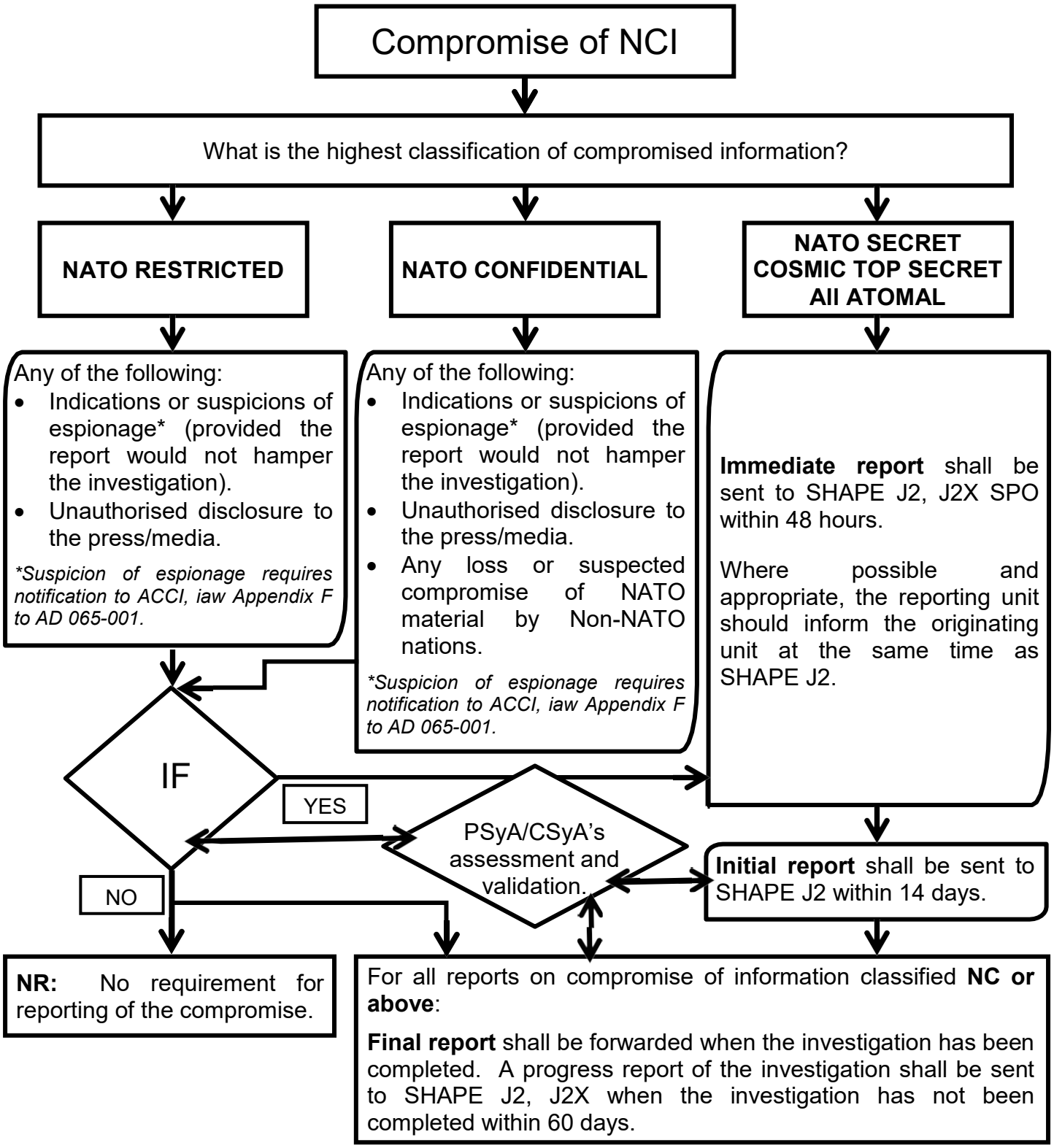
ANNEX Y TO
AD 070-001
DATED 22 DEC 21

SECURITY PROCEDURES FOR PHASE II – INVESTIGATION OF A BREACH OF SECURITY



ANNEX Z TO
AD 070-001
DATED 22 DEC 21

SECURITY PROCEDURES FOR PHASE III – REPORTING OF COMPROMISE



ANNEX AA TO
AD 070-001
DATED 22 DEC 21

BREACH OF SECURITY – INITIAL REPORT

Identifying Reference: .....

DATE: .....

TO: See Distribution

SUBJECT: .....

REFERENCES: A. ACO Directive 070-001 dated .....
B. ACO Directive 065-003 dated .....

PART I

1. **DATE/TIME LOCATION OF INCIDENT:** .....

2. **REPORTED BY:** (Who reported the incident) .....

3. **SUBJECT:** .....
(Full particulars of the individual responsible for the security breach, including svc number, rank, nationality, full name and organisation).

4. **DESCRIPTION OF CLASSIFIED MATERIAL:** .....
(Describe material involved including security classification, originating formation, subject and scope, file reference, copy number and date).

5. **DETAILS OF THE INCIDENT:** .....
(A brief description of what happened, including who, what, where, when, why and how).

PART II

1. **ACTION TAKEN:** .....
(Describe what action where taken to minimise the effects of potential compromise, including the date that a damage assessment was requested from the originator and/or originating organisation).

2. **INVESTIGATING AUTHORITY:** .....
(Identity of the organisation who is investigating the breach of security)

Signature
(Commander or Chief of Staff)

ANNEX:

A. (if applicable).

DISTRIBUTION:
Action:
SHAPE J2, J2X SPO
(as appropriate)
Information:
(as appropriate)

ANNEX BB TO
AD 070-001
DATED 22 DEC 21

BREACH OF SECURITY – FINAL REPORT

Identifying Reference: .....

DATE: .....

TO: See Distribution

SUBJECT: .....

REFERENCES: A (Last report) .....
B. AD 070-001 dated .....

PART III

1. **HISTORY OF EVENTS:** .....
(A chronological summary of all the relevant events).

2. **DAMAGE ASSESSMENT:** .....
(The finalised assessment of the damage resulting from the breach. This will normally be included as an enclosure).

3. **ALLOCATION OF RESPONSIBILITY:** .....
(Investigative conclusion as to whom or what directly contributed to the breach, e.g. human error or negligence and/or established procedure.)

4. **CORRECTIVE ACTION:** .....
(Describe what corrective actions/recommendations were initiated to prevent a recurrence)

5. **COMMANDERS REPORT:** .....
(Details of executive action including the commander's opinion as to individual responsibility, and the remedial action taken. If applicable, why remedial and corrective actions have not been taken and if applicable, a request for relief from accountability for any missing material).

Signature
(Commander or Chief of Staff)

Enclosure(s): (if applicable)

DISTRIBUTION:

Action:

SHAPE J2 J2X SPO
(as appropriate)

Information:

(as appropriate)

ANNEX CC TO
AD 070-001
DATED 22 DEC 21

ACO SECURITY INSPECTION CHECKLIST
by the ACO Security Inspection Team on the Inspection of the Security Arrangements
for Security of NATO Classified Information at the HQ

PART I – SECURITY ORGANISATION						
		U	**M**	**S**	**G**	**Yes/No/NA and Comments**
Corrective Actions / Recommendations from last security inspection report affecting the HQ Security Organisation.						
Have the Corrective Actions / Recommendations from the last security inspection report been implemented (if not, why not).						
1.	HQ Security Office: a. Is the HQ Security Office formally established? b. Is the HQ Security Officer appointed? c. Does HQ Security Officer have a deputy and sufficient specialist and administrative staff to fulfil his responsibilities? d. Are members of the HQ Security Office adequately trained to carry out their duties?					
2.	Have the following been formally appointed: a. HQ COSMIC and ATOMAL Control Officer (HQ CACO)? b. Divisional Security Officers (DSOs)? c. Branch Security Officers (BSOs)? d. Division Document Control Officers (DDCOs)? e. Are the appointed HQ CACO, DSOs, BSOs, and DDCOs adequately trained to carry out their duties?					
3.	Security threat management forum: Is a Security Threat Management Forum established within					

PART I – SECURITY ORGANISATION						
		U	M	S	G	Yes/No/NA and Comments
	the HQ, and is it capable of providing advice and guidance on current threats and countermeasures to the HQ Commander and to subordinated units?					
4.	Previous ACO Inspection or Advisory report: Is the previous security inspection or advisory report available to the HQ Security Officer and to personnel responsible for implementing security within the HQ?					
5.	Is the ACO Security Directive AD 070-001 available for all HQ personnel?					
6.	Is the HQ Supplement to ACO Security Directive AD 070-001 signed by HQ Chief of Staff, promulgated and available to all HQ personnel?					

PART II – PHYSICAL SECURITY						
		U	M	S	G	Yes/No/NA and Comments
Corrective Actions / Recommendations from last security inspection report affecting the HQ Security Organisation.						
Have the Corrective Actions / Recommendations from the last security inspection report been implemented (if not, why not).						
7.	Does the HQ have an Internal Security Plan (ISP), signed by HQ Chief of Staff?					
8.	Does the HQ ISP contain: a. Identification of the assets essential in carrying out of HQ's primary mission, including an assessment of the consequences resulting from the loss of these assets? b. A detailed list of the HQs vital points, including the likely methods of attack against these points?					

PART II – PHYSICAL SECURITY						
		U	M	S	G	Yes/No/NA and Comments
9.	Does the HQ ISP include the following: a. A current threat assessment? b. Identified security measures to be implemented? c. An HQ Incident Response Plan containing: - Identity of HQ personnel responsible for implementing specific measures listed in the plan when decided by the HQ Commander; - Contingency Plan for support and back-up of HQ personnel; - Description of what actions may be undertaken by HQ security forces; - Alternate means of communication for HQ security forces; - Actions and responsibilities upon implementation of each alert state measure; d. HQ Consequence Management Plan, identifying those HQ personnel whose function is to mitigate loss of life or injury to HQ personnel, and damage to HQ property?					
10.	Are exercises conducted (at least once a year) to practice the HQ ISP and are records of such exercises kept for inspection?					
11.	Do the security personnel have necessary Personal Protective Equipment (PPE) required to ensure their safety?					
12.	Is the HQ Main Site protected? a. Is a perimeter barrier established around the site? b. Are Perimeter Intruder Detection System (PIDS) in place? c. Are security cameras established to cover all key areas of the perimeter? d. Are security cameras pan/tilt/zoom and motion					

PART II – PHYSICAL SECURITY						
		U	M	S	G	Yes/No/NA and Comments
	detection enabled? e. Is appropriate security lighting established around the exterior of buildings for night time coverage? f. Is an appropriate access control regime maintained over the entrance to the site? g. Is emergency power supply equipment available to support vital security services?					
13.	Is the HQ Security Centre correctly organised? a. Is the HQ Security Centre adequately manned to efficiently monitor cameras and alarms? b. Is the HQ Security Centre manned on a 24 hour 365 day basis to include holidays? c. Are the camera monitors set up to readily view key areas and any motion detection activation? d. Are security incidents recorded and records retained for later review? e. How long are security incident records retained? f. Does the HQ Security Centre have a 'panic button' linked to the security guard force response capability, or to an appropriate HN law enforcement agency? g. Are SOPs provided to security guards outlining their 'actions-on' in the event of a security incident? h. Are security personnel aware of who to contact in an emergency situation?					
14.	Organisation of Security Areas within HQ: a. Have Security Areas been established within the HQ? b. Are procedures correctly established for controlling access to Security Areas within the HQ? c. Are visitors and regular staff required to wear security passes visibly while present in HQ Security Areas?					

PART II – PHYSICAL SECURITY						
		U	M	S	G	Yes/No/NA and Comments
	d. For visitors' badges, is a distinction made between those visitors with PSC and those without a PSC. e. Are visitors escorted at all times or only in Security Areas? f. Is a record of visitors (including maintenance and cleaning staff) retained? g. Are Class I Security Areas established within HQ? - Is a list of HQ personnel authorised access maintained and displayed at the entrance to Class I Security Areas? - Are satisfactory procedures established for controlling access to Class I Security Areas? - Are combination locked doors in place? - Are alarms and CCTV systems in place?					
15.	NATO Classified Registry: a. Does the HQ have a Classified Registry? b. Is the HQ Classified Registry correctly established within a Class I Security Area?					
16.	Storage of NATO Classified Material: a. Are appropriate security containers provided for storage of material classified NATO CONFIDENTIAL and above? b. Are checks of security containers in which classified material is held carried out at the end of work and out of duty hours (ACO Forms 77 and 79)? c. Are appropriate combination locks provided? d. Are keys and combinations adequately protected? e. Are combinations changed as a minimum every 12 months? f. Are records retained of combination changes? g. Are combination envelopes properly protected?					

PART II – PHYSICAL SECURITY						
		U	M	S	G	Yes/No/NA and Comments
	h. Are combination envelopes classified NATO SECRET or higher logged in the classified registry system?					
17.	Ancillary Staff (cleaners and maintenance staff): a. Are ancillary staff provided by a security cleared company? b. Are the individuals security cleared? c. Are these staffs escorted on a permanent basis while on the HQ premises?					
18.	Intruder and environmental Alarms: a. Does the HQ ISP or supporting SOPs clearly state the regime for testing alarm systems: - The frequency of tests; - The procedures for testing alarms; - The procedures for reacting to an alarm activation. b. What is the reaction time for an intruder response guard force? c. How often is the guard force response to an intruder incident tested, and when was the last documented test?					
19.	Physical Security Checks: a. Are HQ personnel aware of the requirement to ensure offices they are responsible for are secured at cease work, and that: - All classified material is to be locked away; - Computers are to be switched off. b. Are internal security checks carried by HQ Security Office personnel outside of normal hours (evenings, nights, weekends, public holidays)?					
20.	Technical Security Checks: a. Are arrangements in place for technical security checks (e.g., sweeps) to be carried out in conference rooms					

PART II – PHYSICAL SECURITY						
		U	M	S	G	Yes/No/NA and Comments
	and senior management office areas, or other areas that are deemed to be sensitive? b. Are conference rooms or other areas secured following technical security checks? c. Is a record of technical security checks maintained?					
21.	Security Pass System: a. Is the HQ security pass system established? b. Is the HQ Security Pass Office established and supervised by the HQ Security Office? c. Are Standard Operational Procedures or other instructions in place to direct the requirements of the HQ Security Pass Office?					
22.	Emergency and Contingency Planning: a. Are emergency and evacuation procedures clearly documented? b. Are HQ personnel aware of the emergency/evacuation procedures? c. Are emergency and evacuation procedures exercised?					

PART III – PERSONNEL SECURITY						
		U	M	S	G	Yes/No/NA and Comments
Corrective Actions / Recommendations from last security inspection report affecting the HQ Security Organisation.						

PART III – PERSONNEL SECURITY						
		U	M	S	G	Yes/No/NA and Comments
Have the Corrective Actions / Recommendations from the last security inspection report been implemented (if not, why not).						
23.	Are all HQ personnel who require access to information classified NATO CONFIDENTIAL and above appropriately cleared?					
24.	Are processes for re-validation of Personnel Security Clearances established prior to expiration date?					
25.	Use of ACO Form 107 within HQ: a. Is the ACO Form 107 used in HQ? b. Are copies of Personnel Security Clearance Certificates attached to ACO Forms 107? c. Is the identification of need-to-know procedure established for granting HQs' personnel with access to NATO Classified Information? d. Are initial security briefings provided to all HQ personnel, signed by briefed individuals and countersigned by briefers? e. Are initial ATOMAL security briefings provided by HQ CACO to personnel authorised by the HQ Commander to have access to ATOMAL information, signed by briefed individuals and countersigned by the briefer? f. Are annual ATOMAL security briefings provided by the HQ CACO to personnel authorised by the HQ Commander to have access to ATOMAL information, signed by briefed individuals and countersigned by the briefer? g. Are annual general security briefings provided to all HQ personnel? h. Are the certificates of final security briefings (and debriefings) signed by all HQ personnel at the end of their					

PART III – PERSONNEL SECURITY						
		U	M	S	G	Yes/No/NA and Comments
	tour of duty in the HQ, and countersigned by briefers? i. Are the certificates of final security briefings (and debriefings) signed by the HQ personnel authorised by the HQ commander to have access to ATOMAL information and countersigned by HQ CACO?					
26.	Does the HQ Security Office maintain the database of security infractions/incidents?					
27.	Are records of security infractions/incidents kept in personnel security files?					
28.	Are procedures clearly stated to indicate escalatory actions for repeat security offenders?					
29.	Are personnel security files correctly maintained to include up-to-date and relevant security information?					

PART IV – SECURITY OF INFORMATION						
		U	M	S	G	Yes/No/NA and Comments
Corrective Actions / Recommendations from last security inspection report affecting the HQ Security Organisation.						
Have the Corrective Actions / Recommendations from the last security inspection report been implemented (if not, why not).						
30.	Is COSMIC TOP SECRET and ATOMAL (CTS/A) information stored and administered in the HQ in accordance with NATO standards? a. Have CTS/A Sub-Registry and Control Points (CPs) been established within the HQ? b. Is the HQ Sub-Registry authorised to destroy ATOMAL material.					

PART IV – SECURITY OF INFORMATION						
		U	M	S	G	Yes/No/NA and Comments
	c. Does the HQ CTS/A Sub-Registry and CPs maintain bound paper logbooks, separate for COSMIC and for ATOMAL material handled? d. Are the bound paper COSMIC and ATOMAL logbooks approved for use by the HQ Security Authority and HQ CACO? e. Is CTS/A material stored and administered separately from NATO SECRET and below? f. Is each CTS and ATOMAL document kept in separate, colour coded folders, together with all accompanying documentation (e.g. copy of receipt, disclosure sheet, destruction form, downgrading decision)? g. Is CTS/A material disseminated in accordance with listings of authorised recipients? h. Are receipts obtained for CTS/A material? i. Does the HQ CACO maintain lists and specimen signatures of individuals authorised access to CTS/A material? j. Is the list and specimen signatures of individuals who are authorised access to CTS/A material annually reviewed by the HQ CACO to ensure individuals retain the 'need-to-know' and have a valid security clearance? k. Is CTS/A material transmitted exclusively through the ACO CTS/A Registry System? l. Do generated ATOMAL documents contain the mandatory statement concerning safeguarding? m. Are control numbers assigned to all CTS/ ATOMAL documents? n. Do 'Disclosure Sheets' exist for each individual CTS and ATOMAL document, which are attached to the					

PART IV – SECURITY OF INFORMATION						
		U	M	S	G	Yes/No/NA and Comments
	document; are the disclosure sheets signed on each annual inventory and HOTO of the HQ COSMIC Control Officer (CCO)? o. Are the disclosure sheets retained, on destruction of the document, with the destruction certificates? p. Is the initial receipt of CTS/A information processed only by the HQ CCO or an alternate? q. Are CTS/A documents returned to the HQ Sub-Registry or CP, which hold them on charge for destruction? r. Is destruction of ATOMAL material effected by HQ CCO in collaboration with the HQ CACO and an independent witness? s. Are the annual inventories of CTS and ATOMAL information conducted satisfactorily (100%, physical presence, page count) and are the reports submitted to ACO Security Authority up to the end of January each year, and copies of reports retained? t. Are CTS and ATOMAL documents held within the HQ subject to quarterly 25% spot-checks by the HQ CACO, and records (QSRs) retained? u. Has the HQ developed a program of annual revision of CTS and ATOMAL information by originators in order to decide further course of action (e.g. destruction, downgrading or retention)? v. Is the process of annual revision of CTS and ATOMAL material initiated by the HQ CACO and supervised by the HQ Security Authority?					
31.	Is NATO SECRET (NS) information stored and administered in HQ in accordance with NATO standards? a. Is a NATO SECRET Registry established within the					

PART IV – SECURITY OF INFORMATION						
		U	M	S	G	Yes/No/NA and Comments
	HQ with trained personnel with assigned responsibilities? b. Are appropriate control records maintained of NS documents (e.g. bound paper logbook, receipts, destruction certificates, retention of control records)? c. Are all transactions involving NS documents covered by signed receipts? d. Are changes to NS documents disseminated and controlled as separate documents until incorporated into the basic documents? e. Are the NS documents subject to annual inventory and records retained? f. Are the NS documents subject to periodic spot-checks and records retained? g. Is it possible to establish who has had access to the NS documents (e.g. access sheets, signing logbooks, personal holdings cards); are these retained for specific period of time?					
32.	Procedures for destruction of NATO Classified documents: a. Is the systematic programme in effect for the destruction of classified documents, which are no longer required by the HQ? b. Are exercise classified messages destroyed at the completion of the exercise? c. Are procedures for destruction of NATO classified documents established? d. Is approved equipment used for destruction of classified documents? e. Are destruction certificates raised for documents classified NS and above?					

PART IV – SECURITY OF INFORMATION						
		U	M	S	G	Yes/No/NA and Comments
	f. Are destruction certificates for NS material appropriately signed by both the person destroying the document/material and independent witness? g. Are destruction certificates retained for specific period of time?					
33.	Reproduction of NATO Classified Documents: a. Is the number of reproductions of NS documents and their copy numbers recorded by the registry? b. Are Multi-Function Devices (MFDs), photocopiers or printers available in open areas? c. Is access to MFDs, photocopiers and printers controlled by cards or access code?					
34.	Transmission of NATO classified documents: a. Are procedures clearly documented for: - the transmission of NATO classified documents; - personal hand carriage of NATO classified documents; - using the ACO courier system; - international transmission; - protection of the HQ's NATO Seals?					
35.	Is a NATO courier certificate used for transmission of NATO classified material?					
36.	Has the HQ Commander designated, in written, the custodian responsible for the HQ's NATO Seals?					
37.	Has the custodian signed for HQ's NATO Seals?					
38.	Are the HQ's NATO Seals registered as NATO SECRET documents?					
39.	Are folders and file covers used to store NATO classified documents and are they properly colour coded?					

PART V – INFORMATION AND INTELLIGENCE SHARING WITH NON-NATO ENTITIES (I&IS with NNEs)						
		U	M	S	G	Yes/No/NA and Comments
Corrective Actions / Recommendations from last security inspection report affecting the HQ Security Organisation.						
Have the Corrective Actions / Recommendations from the last security inspection report been implemented (if not, why not).						
40.	Has the HQ Delegated Authority (DA) been formally appointed by the ACO Security Risk Owner?					
41.	Has an HQ Principle Security Advisor (PSyA) been formally appointed?					
42.	Are procedures for I&IS with NNEs within the HQ clearly documented?					
43.	Are control records retained for all classified information released to Non-NATO recipients?					
44.	Are protective marking requirements clearly documented and applied?					
45.	For each NNE individual working within the HQ, does a written decision by the HQ DA exist (Annex H), which details physical access to HQ Security Areas, access to CIS, and access to NATO classified information that is non-released?					
46.	For each NNE individual working within the HQ does an Annex L exist, signed by divisional CIS Coordinator, which details technical restrictions to be applied for access to the NSWAN?					
47.	For an NNE individual with NSWAN access, was their account built in accordance with the technical restrictions described in the relevant Annex L?					
48.	Does the HQ CIS Security Officer do periodic checks to ensure NSWAN accounts for NNE individuals continue to					

PART V – INFORMATION AND INTELLIGENCE SHARING WITH NON-NATO ENTITIES (I&IS with NNEs)						
		U	M	S	G	Yes/No/NA and Comments
	only have access to NATO classified information necessary to do their job?					
49.	Has the Annual Security Report (ASR) on I&IS with NNEs been provided (including subordinated HQs and HQ led-Operations) to the ACO Security Authority at SHAPE?					
50.	Do the HQ Security Office hold all the decisions (Annexes H together with Annexes L) taken by HQ DA on I&IS with NNEs?					
51.	Is the ID/access badge for each NNE individual, granted access to an HQ Security Area, distinctly different from the ID/access badge for NATO staff members?					
52.	Has each NNE individual with granted access to NATO classified information signed an acknowledgement of responsibilities for the protection of NATO classified information; and is the acknowledgement re-signed annually?					

PART VI – SECURITY PROCEDURES						
		U	M	S	G	Yes/No/NA and Comments
Corrective Actions / Recommendations from last security inspection report affecting the HQ Security Organisation.						
Have the Corrective Actions / Recommendations from the last security inspection report been implemented (if not, why not).						
53.	Is a database of security infractions maintained by HQ Security Office?					
54.	Are copies of security infractions maintained on the personnel security files?					

PART VI – SECURITY PROCEDURES						
		U	M	S	G	Yes/No/NA and Comments
55.	How many security infractions have occurred since previous inspection: a. Affecting COSMIC TOP SECRET / ATOMAL information; b. Affecting NATO SECRET information; c. Affecting NATO CONFIDENTIAL information.					
56.	Is this an increase or decrease over previous period:					
57.	Have appropriate reports been provided to ACO J2X at SHAPE: a. Immediate report - within 48 hours - In cases where lost or compromised NATO classified material involves NATO SECRET, COSMIC TOP SECRET or ATOMAL information; - In case when there are indications or suspicions of espionage, unauthorised disclosure to press/media has occurred or any loss or suspected compromise of NATO material by Non-NATO Entity individual; b. Initial report - within 14 days c. Final report - within 60 days					
58.	Have all security infractions been successfully investigated?					
59.	Have damage assessments been done by the Originator of compromised information and were all recipients informed?					
60.	Was the security investigation closed by the relevant Confirming Authority?					
61.	Was the write off of lost NATO classified material authorised by the relevant Confirming Authority?					
62.	From interrogation of records is it possible to identify if an individual is a repeat offender over a period of time?					

PART VI – SECURITY PROCEDURES						
		U	M	S	G	Yes/No/NA and Comments
63.	Is appropriate administrative/disciplinary action taken against violators and are records maintained?					
64.	Do the HQ procedures clearly state the escalatory actions required to deal with repeat security offenders?					
65.	Are records of security investigation reports and details of remedial and corrective actions taken, held for a minimum of three years?					
66.	Does the HQ prepare an annual security Programme Of Work (POW) that includes planned security inspections of subordinated unit? Is the security POW provided to the ACO J2X at SHAPE prior to the end of October each year?					
67.	Does the HQ properly prioritise the inspection of its subordinate units according to their individual categories?					
68.	Are completed inspection reports forwarded to SHAPE ACOS J2, within the required 45-day time limit following the inspection?					

PART VI – SECURITY PROCEDURES						
		U	M	S	G	Yes/No/NA and Comments
Corrective Actions / Recommendations from last security inspection report affecting the HQ Security Organisation.						
Have the Corrective Actions / Recommendations from the last security inspection report been implemented (if not, why not).						
69.	Is the HQ Security Awareness Officer appointed?					

PART VI – SECURITY PROCEDURES						
		U	M	S	G	Yes/No/NA and Comments
70.	Does the HQ have a progressive Security Awareness and Education Programme, approved by HQ Chief of Staff?					
71.	Is the Security Awareness and Education Programme supported by HQ senior management staff?					
72.	Are HQ senior management staff aware of their security responsibilities?					
73.	Are newcomers provided with induction security briefings on arrival at the HQ, before being granted access to NATO Classified Information?					
74.	Are all HQ personnel provided with annual security briefings?					
75.	Does the initial and annual security briefings address all aspects of security: a. Physical Security; b. Personnel Security; c. Security of Information; d. Security Procedures; e. Information and Intelligence Sharing with Non-NATO Entities; f. Industrial Security; g. CIS Security.					
76.	Are all HQ personnel provided with final security briefings (de- briefings) at the end of their tour of duty in the HQ?					
77.	Are HQ personnel authorised to have access to ATOMAL information provided with specific initial and annual briefings, addressing control procedures and special handling requirements?					
78.	Are HQ personnel authorised by the HQ Commander to have access to CTS and ATOMAL information provided with de-briefings when such access is no longer required?					

PART VI – SECURITY PROCEDURES						
		U	M	S	G	Yes/No/NA and Comments
79.	Are the HQ staff members aware of to whom they should report security concerns?					
80.	Are All Users Messages provided periodically on topical security issues?					
81.	Are periodic briefings given to groups of staff members by HQ security personnel or external security SMEs?					
82.	Are security posters addressing specific security available and are they displayed within the HQ to draw the attention of all HQ personnel and visitors to the building(s)?					
83.	Does the HQ Security Office maintain statistics on the type and frequency of security violations and breaches of security in order to develop appropriate and relevant security awareness and education material?					
84.	Does the HQ provide security awareness and education material to its subordinate elements?					
85.	Is awareness and educational material accessible for all staff members?					
86.	Are unqualified HQ security appointed personnel nominated to attend the NATO School Oberammergau Security Course?					
87.	How many HQ security appointed personnel attended the NATO School Security Course since the last inspection?					
88.	Do personnel in security posts such as HQ CACO/DSOs attend the ACO Security Course held annually by ACO J2X at SHAPE?					
89.	Are Security Newsletters, Security Flyers and other security awareness documents promulgated inside the HQ and to subordinate units?					
90.	Are Security Workshops organised and performed in the HQ?					

PART VI – SECURITY PROCEDURES						
		U	M	S	G	Yes/No/NA and Comments
91.	Are the Quarterly Security Returns signed by the HQ Security Authority and sent on time to the ACO Security Authority?					

ANNEX DD TO
AD 070-001
DATED 22 DEC 21

REPORT

on Inspection of Security Arrangements for Protection of NATO Classified Information in ……..

Part I – INSPECTION SUMMARY

GENERAL

1. In compliance with the provisions set forth in NATO security policy, the…….. (Security Authority) inspecting team carried out this inspection of the security arrangements for the protection of NATO classified information in…..……

Date of Inspection	
(rank, name)	Team Leader
	Security Organisation
	Physical Security
	Personnel Security
	Security of Information
	Information and Intelligence Sharing with Non-NATO Entities
	Security Procedures
	Security Awareness and Education
	CIS Security

2. The programme of the security inspection included the following:

a. Introductory meeting with presence of HQ commander (or his nominated representative);
b. General discussions with the HQ Security Officer;
c. Inspection of the security arrangements within headquarter;
d. Verbal report to the commander of the inspected headquarter (or his nominated representative).

PREVIOUS INSPECTION

Date of Previous Inspection	
Report Reference	
Corrective Actions / Recommendations from the Previous Inspection	
Security Organisation	
Physical Security	
Personnel Security	
Security of Information	
Information and Intelligence Sharing with Non-NATO Entities	
Security Procedures	
Security Awareness and Education	
CIS Security	

3. The corrective actions and recommendations from the previous inspection were addressed by the inspection team during the course of the inspection.

HEADQUARTER'S STAFF INVOLVED IN THE INSPECTION

(name, rank, post title)	HQ Commander or his nominated representative
	HQ Security Officer
	Security Organisation
	Physical Security
	Personnel Security
	Security of Information
	Information and Intelligence Sharing with Non- NATO Entities
	Security Procedures

INTRODUCTORY MEETING

4. The inspection team leader introduced the team and addressed the main aspects to be covered during the inspection. The HQ commander (or his nominated representative) introduced the HQ security personnel responsible for implementation of NATO security standards and presented general security organisation of the HQ.

VERBAL REPORT

5. The inspection team leader presented to HQ commander (or his nominated representative) a verbal report of the inspection. This report addressed the following corrective actions (if applicable) and main recommendations and observations arising from the inspection.

CORRECTIVE ACTIONS (if applicable)

6. The following corrective actions are required in order that NATO classified information is protected in accordance with ACO Security Directive AD 070-001.

Security Organisation	
Physical Security	
Personnel Security	
Security of Information	
Information and Intelligence Sharing with Non-NATO Entities	
Security Procedures	
Security Awareness and Education	
CIS Security	

7. A corrective action report is to be provided by …….. (HQ) to the …… (inspecting Security Authority) within 30 days of the date of this report, indicating the actions which have been initiated and the expected timescale for their completion.

RECOMMENDATIONS

8. The following recommendations and observations were made in order to maintain or enhance the current security posture.

CONCLUSION

9. The security arrangements in ……..… (HQ) for the protection of NATO classified information are overall ……..… (GOOD / SATISFACTORY / MARGINAL /

UNSATISFACTORY). Specific attention should be given to ……..…

10. (if applicable) The inspection team leader highlighted the positive contribution of the HQ Security Officer and his staff, and stressed the importance of maintaining the support of Command Group to protection of NATO classified information.

Part II – INSPECTION DETAILS

11. Attached at Annexes to this report are the completed inspection Security and CIS Security checklists addressing the security aspects covered during the course of the inspection.

ANNEX EE TO
AD 070-001
DATED 22 DEC 21

GENERAL RESPONSIBILITIES

NATO NATIONS

1. Each NATO Nation will:

a. Designate one or more security authorities responsible to the NSA, as appropriate. The Designated Security Authority (DSA) will be responsible for communicating national and NATO security policy to industry and for providing direction and assistance in its implementation; in some countries there may be more than one authority designated as a DSA, or the function of a DSA may be carried out by the NSA:

b. Certain functions of the NSA/DSA may be carried out by other competent security authorities in accordance with national laws and regulations.

c. Ensure that it has the means to make its industrial security requirements binding upon industry and that NSA/DSA/SAA have the right to inspect and approve the measures taken in industry for the protection of NCI.

d. Determine, as appropriate, the aspects of a NATO contract or sub-contract requiring security protection and the security classification to be accorded to each aspect.

e. Prior to the release of NCI to a Contractor, prospective Contractor, or Sub-contractor, the NATO Nation will ensure that the Contractor(s), prospective Contractor(s), or Sub-contractor(s) and their facility(ies) have the capability to protect NCI adequately, in accordance with NATO Security Policy, and with national laws and regulations.

f. Grant a FSC to the facility/facilities.

g. If appropriate grant a NATO PSC to all eligible personnel whose duties require access to information classified NC or above.

h. Ensure that access to NCI is limited to those persons who have a need-to-know for purposes of performance on the NATO project, programme and/or construction.

i. Make arrangements whereby persons considered by the NSA/DSA to be a security risk can be excluded or removed from positions in which they might endanger the security of NCI.

j. Ensure the implementation of the NATO procedures for the mutual safeguarding of the secrecy of inventions, as and when necessary.

k. Provide, upon request to an NSA/DSA of a NATO nation, or to a NATO civil or military body, an FSCC to enable a facility falling within its security cognisance to negotiate or fulfil a contract/sub-contract involving information classified NC or above.

l. Provide, upon request, to a NSA/DSA of another NATO Nation, or a NATO civil or military body (e.g. ACO component), an FSCC to enable a facility falling within its security cognisance to negotiate or fulfil a contract/sub-contract involving information NC or above.

m. Provide, upon request, to a NSA/DSA of another NATO Nation, or a NATO civil or military body (e.g. ACO component), a PSC for the persons for whom it has security responsibilities to enable them to fulfil a NATO classified contract.

n. Take action with regard to the specific arrangements to be carried out in matters of transportation and international visits in accordance with the requirements of NATO Security Policy.

o. Investigate all cases in which it is known, or where there are grounds for suspecting, that NCI has been lost or compromised. Each NATO Nation will comply with the investigative requirements set out in NATO Security Policy and its supporting directives, and promptly inform the ACO component APO, the NATO Nations concerned and if applicable the NOS, of the details of any such occurrences.

p. Ensure that for any facility in which NCI is to be used, a person or persons will be appointed, where appropriate, in accordance with national laws and regulations, to effectively exercise the responsibilities for safeguarding NCI. These officials will be responsible for limiting access to the NCI involved in a contract to those persons who have been security cleared and have a clear need-to-know.

SECURITY COMMITTEE

2. The Security Committee will:

a. Monitor the implementation of the NATO Security Policy and make appropriate recommendations to the NAC for the improvement of the security protection of NCI entrusted to industry; and

b. Consider matters of industrial security referred to it by the NAC, a NATO Nation, the Secretary General, the NATO Military Committee (NAMILCOM), ACO and heads of other NATO Civil and Military bodies.

NATO OFFICE of SECURITY (NOS)

3. The NOS will:

a. Assist and give guidance in industrial security matters to NPA/NPOs and such other NATO industrial projects as may be designated by the NAC and supervise the implementation of NATO Security Policy in those organisations and projects.

b. In agreement with the NSAs/DSAs of NATO Nations concerned, assist and give guidance to other NSAs/DSAs in the implementation of NATO Security Policy in connection with the activities of NPA/NPOs.

c. In agreement with the NSAs/DSAs of member nations concerned, assist and

give guidance on NATO security policies and directives to facilities participating in the activities of NPA/NPOs.

d. Make periodic inspections of the security arrangements for the protection of NCI in NPA/NPOs.

e. With the agreement of the appropriate NSA/DSA, make periodic examinations of the security arrangements for the protection of NCI in the NATO Nations.

f. Give guidance and advice, when requested by NSAs/DSAs, on matters of industrial security arising in all NATO related projects.

SHAPE SEM J2X

4. The SHAPE SEM J2X shall:

a. Assist and provide guidance in industrial security matters to APOs responsible for the management of ACO component led classified programmes, projects and/or constructions, and supervise the implementation of basic principles and minimum standards of NATO Security Policy, ACO CIS Security Directive AD 070-005 and this ACO Security Directive in APOs and their classified programmes, projects and/or constructions.

b. Conduct an annual review of implemented security arrangements for the protection of NCI in APO led classified programmes, projects and/or constructions.

ALLIED COMMAND COUNTERINTELLIGENCE (ACCI)

5. ACCI shall:

a. Provide CI protection of ACO led programmes, projects and/or constructions involving NCI.

b. Open, conduct, and close CI investigations related to ACO led programmes, projects and/or constructions involving NCI.

c. Control and monitor all CI investigations in tandem with the Allied CI Coordinating Authority (ACCA).

d. Coordinate with both the Host Nation NSA/DSA and the sending nation NSA/DSA of the suspected violator.

e. Collect CI evidence in accordance with the applicable criminal procedure rules of the NATO Nations involved.

f. Work closely with APO Security Managers to quickly determine whether a security violation or breach should result in an ACCI investigation.

g. Advise APO Security Managers on the protection and safeguarding procedures for evidence.

h. Respond to APO Security Managers notifications as quickly as possible and

provide an assessment of whether a CI investigation needs to be conducted.

i. Advise APO Security Managers as to the safeguarding and confidentiality of information regarding security breaches related to classified programmes, projects and/or constructions.

j. Provide respective APO Security Managers periodic updates relating to the CI investigation, allied with the final determination..

k. Limit the distribution of sensitive CI investigative details only to those parties with a clear need-to-know.

ACO PROGRAMME/PROJECT/CONSTRUCTION OFFICES

6. Each APO with project management responsibilities designated by the commander of an ACO component will be bound by the general security regulations laid down in NATO Security Policy, ACO CIS Security Directive, this ACO Security Directive and any other ACO security regulations as may apply. Each APO shall:

a. Draw up the implementing security regulations for the classified programme, project and/or construction in compliance with the provisions of NATO Security Policy, ACO CIS Security Directive, this ACO Security Directive and any other ACO security regulations and subsequently supervise the enforcement of the security regulations.

b. In conjunction with the NSAs/DSAs concerned and SHAPE SEM J2X co-ordinate the implementation of NATO Security Policy, ACO CIS Security Directive, this ACO Security Directive and any other ACO security regulations, both by potential Contractors and by Contractors, and deal with any security problems arising in any NATO classified programme, project and/or construction in which the APO is engaged.

c. Take action as required, and in accordance with the provisions of this ACO Security Directive, in respect of the special arrangements for International Visits.

d. Be responsible for preparing the Project Security Instruction for the programme, project and/or construction they manage for approval by the relevant NSAs/DSAs.

e. Be responsible for raising a Transportation Plan as identified in the PSI.

ANNEX FF TO
AD 070-001
DATED 22 DEC 21

FACILITY SECURITY CLEARANCE INFORMATION SHEET (FSCIS)

Introduction

1. Attached is a sample format of a Facility Security Clearance Information Sheet (FSCIS) for the quick exchange of information between a National Security Authority (NSA) or a Designated Security Authority (DSA) or other competent national security authorities and NATO contracting authorities (e.g. APOs) with regards to the Facility Security Clearance (FSC) of a facility involved in classified tenders, contracts or sub-contracts.

2. The FSCIS is not for use by Contractors.

3. The FSCIS is divided into a request and reply section, and can be used for the purposes identified above, or for any other purposes for which the FSC status of a particular facility is required. The reason for the enquiry must be identified by the requesting APO in form field 7 of the request section.

4. The details contained in the FSCIS shall normally not be classified and therefore the preferable way for the exchange of the FSCIS will be electronically between the respective NSAs/DSAs/APOs.

5. NSAs/DSAs should make every effort to respond to a FSCIS request within 5 working days. In urgent cases, an NSA/DSA will send the response within 3 working days.

Procedures for the Use of the Facility Security Clearance Information Sheet

	The Requesting APO (inserts full ACO component name)
1. Request Type	The requesting APO selects the appropriate checkbox for the type of FSCIS request. Include the level of security clearance requested. The following abbreviations should be used: **TS** - National TOP SECRET **CTS** - COSMIC TOP SECRET **S** - National SECRET **NS** - NATO SECRET **C** - National CONFIDENTIAL **NC** - NATO CONFIDENTIAL **CIS** - Communication and Information Systems for processing classified information An FSC is not required for access to, or generation of information classified NR; however, some NATO Nations require a FSC for Contractors/Sub-contractors under their jurisdiction, for access to information classified NR.
2. Subject Details	Form Fields 1 through 6 are self-evident. Form Field number 5 is optional.

3. Reason for Request	Give the specific reason for the request, provide programme/project /construction indicators, number of contract, letter of intent or invitation. Please specify the need for storage capability, CIS classification level, etc. Any deadline/expiry/award dates, which may have a bearing on the completion of a FSC, should be included.
4. Requesting APO	State the name of the actual APO requestor and the date of the request by using the dd/mm/yyyy format.
5. Reply Section	Form Field 1-6: Select appropriate fields. Form Field 2: In case an FSC is in progress it is essential to give the APO requestor an indication of the required processing time (if known). Form Field 6: (a) The validation date inputted will be either when the FSC for the Contractor's facility expires, and/or when this FSCIS expires (if different). Any date inputted must be in the dd/mm/yyyy format. It should be noted that some NATO Nations do not have an expiry date for FSCs or the FSCIS, so will be marked 'N/A'". (b) Should an FSC and/or FSCIS expire prior to the award of a NATO Classified Contract the requesting APO is responsible for submitting a new FSCIS request to the NSA/DSA of the Contractor to re-validate the FSC of the facility.
6. Remarks	May be used for additional information with regard to the FSC, the facility or the foregoing Items.
7. Issuing NSA/DSA	State the name of the providing authority (on behalf of the NSA/DSA) and the date of the reply by using the dd/mm/yyyy format.

APPENDIX 1 TO
ANNEX FF TO
AD 070-001
DATED 22 DEC 21

FACILITY SECURITY CLEARANCE INFORMATION SHEET

All fields must be completed and the form communicated via ACO component-to-Government channels

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: [ ] TS [ ] CTS [ ] S [ ] NS [ ] C [ ] NC
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, sub-contract, programme/project):
……

Requesting APO: 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.
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*)....…….

ANNEX GG TO
AD 070-001
DATED 22 DEC 21

CONTRACT SECURITY CLAUSE

For Inclusion in Tenders and Contracts Involving Information Classified NATO RESTRICTED

AD 070-001

INTRODUCTION

1. This contract security clause is published by the Security Committee (AC/35) in support of NATO Security Policy, C-M(2002)49, and its supporting directives.

BACKGROUND

2. This contract security clause contains rules and regulations that shall be applied by the Contractor addressing the minimum security requirements for the protection of NATO RESTRICTED (NR) information received or produced by it as a result of the contract. This security clause addresses all aspects of security (personnel security, physical security, security of information, Communication and Information System (CIS) Security, and industrial security) that the Contractor is required to implement.

3. This contract security clause forms part of the contract and shall provide direction to ensure compliance by Contractors on the protection of NR information.

SECTION I - RESPONSIBILITY

4. Contractors handling and/or storing NR information shall appoint an individual of suitable seniority who shall act as the Security Officer (SO) of the facility with responsibility for ensuring the protection of NR information in compliance with the provision of this security clause and any other additional requirements advised by the Contracting Authority. The SO shall also act as the point of contact with the Contracting Authority, or if applicable with the National Security Authority (NSA) or Designated Security Authority (DSA).

SECTION II - PERSONNEL SECURITY

5. A Personnel Security Clearance (PSC) is not required for access to information classified NR. Individuals who require access to NR information shall be briefed on security procedures and their responsibilities by the nominated SO, have a need-to-know and acknowledge in writing that they fully understand their security responsibilities and the 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 facility security officer.

SECTION III - PHYSICAL SECURITY

6. NR information shall be stored in a locked container that deters unauthorised access; such as a locked desk or cabinet, or in a room or area to which access is controlled (hereinafter referred to as Administrative Zone[52])

7. NR information shall be handled in Administrative Zones or held under personal custody.

[52] An Administrative Zone may be established around or leading up to NATO Class I or Class II Security Areas. Such a zone requires a visibly defined perimeter within which the possibility exists for the control of individuals and vehicles. Only information classified up to and including NR shall be handled and stored in Administrative Zones.

SECTION IV - SECURITY of INFORMATION

Control and Handling

8. Unless a NATO Nation has specifically mandated contractors under their jurisdiction to do so, NR information is not required to be individually recorded or processed through a Registry System.

Access

9. Access to NR information shall be granted only to personnel involved in the contract who fulfil the conditions according to Paragraph 5 (above).

Reproduction

10. Documents, extracts, and translations of information classified NR may be reproduced by individuals authorised for access to the information and on equipment with controlled access.

Destruction Requirements

11. NR information shall be physically destroyed in such a manner that ensures it cannot be reconstructed in full or in part.

12. Destruction of reproduction equipment utilising electronic storage media shall be in accordance with the applicable requirements in section VI.

Packaging

13. Information classified NR shall, as a minimum, be transmitted in a single opaque envelope or wrapping. The markings on the package shall not reveal that it contains information classified NR.

Carriage/ Movement within a Contractor's Facility

14. NR information carried within the perimeter of the site or establishment shall be covered in order to prevent observation of its contents.

National/International Transfer

15. The carriage of NR material shall, as a minimum, be in a single opaque envelope or packing (no marking shall be visible on the outer envelope) and may be:

a. Moved by postal or commercial services;

b. Carried by Contractor personnel; or

c. Transported as freight by commercial services.

Release

16. NR shall not be released to entities not involved in the contract without the prior approval of the contracting authority.

Security Incidents

17. Any Incident, which has or may lead to NR information being lost or compromised, shall immediately be reported by the SO to the Contracting Authority.

SECTION V - SUB-CONTRACTING

18. Sub-contracts shall not be let without the prior approval of the Contracting Authority.

19. Sub-contractors shall be contractually obliged to comply with the provisions of this document and any other additional security requirements issued by the Contracting Authority.

Notification of Contracts

20. Contractors/Sub-contractors 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.

International Visits

21. 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 (RfV) 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.

SECTION VI - HANDLING OF NATO RESTRICTED INFORMATION ON COMMUNICATION AND INFORMATION SYSTEMS (CIS)

Security Accreditation of Communication and Information Systems

22. Security accreditation shall be performed for all contractors' CIS that are used to handle (store, process or transmit) NR information.

23. This contract security clause contains the rules and regulations that shall be applied by the contractor's SO 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 the Security Aspects Letter associated with the contract.

24. It is the responsibility of the contractor to implement these minimum security requirements when handling NR on its CIS.

25. The SO 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.

26. The following describes the minimum security requirements for handling NR information on contractor's CIS that shall be met:

a. **Identification and Authentication:**

(1) An up-to-date list of authorised users shall be maintained by security management staff.

(2) Credentials shall be established and maintained to identify authorised users.

(3) Users shall themselves authenticate to, and be authenticated by, the system before any access to the CIS will be granted.

(4) Passwords shall be a minimum of 9 characters long and shall include numeric and 'special' characters (if permitted by the system), as well as alphabetic characters.

(5) Passwords shall be changed at least every 180 days. Passwords shall be changed as soon as possible if they have, or are suspected to have been compromised or disclosed to an unauthorised person.

(6) The re-use of a number of previous passwords shall be denied.

(7) The system shall provide only limited feedback information to the user during the authentication process.

(8) Accounts that are no longer required shall be locked or deleted.

(9) When the authentication of the person is not enforced by physical security measures surrounding the location where the system is installed (e.g. perimeter/building security) or by non-technical security measures surrounding the office areas where components of system are located (e.g. server rooms, user workstation areas), two-factor authentication shall be used.

b. **Access Control:**

(1) The identification and authentication data shall be used by the system to determine user privileges, in accordance with the access control requirements set out in the security related documentation.

(2) From the user account only, it shall be possible for the security management staff to identify the specific user and/or roles.

(3) Mechanisms shall be implemented to restrict access to only that information to support a given project or contract, taking into account the need-to-know principle.

(4) Access to security and system information shall be restricted to only authorised security and system administrators.

(5) Access privileges shall be implemented to restrict the type of access

that a user may be permitted (e.g. read, write, modify, and delete).

(6) The system (e.g. Operating System) shall lock an interactive session after a specified period of user inactivity by clearing or overwriting display devices, making the current contents unreadable and by disabling any user's data access/display devices other than unlocking the activity of the session.

(7) The system shall allow user-initiated locking of the users own interactive session by clearing or overwriting display devices, making the current contents unreadable and by disabling any user data access/display devices other than unlocking the activity of the session.

(8) Security mechanisms and/or procedures to regulate the introduction or connection of removable computer storage media (for example USB, mass storage devices, CD-RWs) to user workstations/portable computing devices shall be implemented.

c. **Security Audit:**

(1) An audit log shall be generated and maintained. System Level, Application Level and User Level events shall be included in the log, as required by the relevant Security Authority as a result of a Risk Assessment. For each of the auditable events, it shall associate individual user identities to those events, and shall include date and time of the event, type of event, user identity, and the outcome (success or failure) of the event. The following events shall always be recorded:

(a) All log on attempts whether successful or failed.

(b) Log off (including time out where applicable).

(c) The creation, deletion or alteration of access rights and privileges.

(d) The creation, deletion or alteration of passwords.

(2) The audit trail and associated archive shall be protected from unauthorised deletion and/or modification; it shall be presented in human readable format either directly (e.g. storing the audit trail in human-readable format) or indirectly (e.g. using audit reduction tools) or both.

(3) Access to audit information shall be controlled; access permissions shall be established to permit access only by the appropriate security management staffs.

(4) The audit data shall be retained for a period agreed by the Contracting Authority, based, where appropriate, on the requirements established by the NSA or DSA.

(5) A means shall be available to analyse and review system activity and audit data, looking for possible or real security violations (analysis may work in support of intrusion detection/ automatic response to an imminent security

violation).

d. **Protection against Malicious Software:**

(1) Virus/malicious code detection software shall be installed on all servers, portable computing devices and workstations dependent upon the vulnerability of the underlying operating system environment. It shall be configured to automatically check on the introduction of removable media (e.g. CDs, USB mass storage devices, flash memory).

(2) The virus/malicious code detection software shall be regularly updated.

e. **Mobile Code:**

(1) The source of the mobile code shall be appropriately verified.

(2) The integrity of the mobile code shall be appropriately verified.

(3) All mobile code shall be verified as being free from malicious software.

(4) Available technical measures shall be enabled to ensure the use of mobile code is appropriately managed. For example, Microsoft Office applications and Internet Browser applications shall be configured to control import/acceptance of mobile code as well as use and creation of mobile code.

f. **Availability**. Security measures ensuring availability of NR information shall be implemented when required by the Contracting Authority.

g. **Import/Export of Data:**

(1) Data transfers between machines, virtual or physical, in different security domains shall be controlled and managed to prevent the introduction of NR data to a system not accredited to handle NR data.

(2) All data imported to or exported from the CIS shall be checked for malware.

h. **Configuration Management:**

(1) A detailed hardware and software configuration control system shall be available and regularly maintained.

(2) Configuration baselines shall be established for servers, LAN Components, Portable Computing Devices and workstations.

(3) Configuration checks shall be made by appropriate Security Management staff on hardware and software to ensure that unauthorised hardware and software has not been introduced.

(4) An inventory of hardware and software should be maintained, with equipment and cabling labelled as part of the inventory.

(5) The configuration of the security enforcing and security relevant functions of the operating system shall only be subject to change by a limited number of authorised system and security administrators.

(6) The security configuration of the operating system shall be maintained with the implementation of the appropriate security patches and updates. Regression Aspects i.e. any potential adverse effects of the modification on existing security measures, shall be considered and appropriate action taken.

(7) The installation and configuration of application software with security relevant or security-enforcing functions shall be subject to a limited number of authorised system and security administrators.

(8) The configuration of the operating system shall be subject to periodic checks to ensure its security compliance.

(9) Changes to the system or network configuration shall be assessed for their security implications/impacts.

(10) The Basic Input/Output System (BIOS) or similar firmware shall be password protected in order to protect access to the system's password data.

i. **Security Management:**

(1) Mechanisms shall be implemented which manage security data and functions; only defined authorised users (or roles) may perform security functions and access security relevant data.

(2) The compromise or suspected compromise of NR information shall be immediately reported for inspection and investigation purposes, through the SO, to the Contracting Authority and, if required by national laws and regulations, to the relevant NSA or DSA.

j. **Approved Products:**

(1) An approved product is one that has been approved for the protection of NR information either by NATO or by the National CIS Security Authority (NCSA) of a NATO Nation or in accordance with national laws and regulations.

(2) The relevant NSA, NCSA or DSA shall be consulted, through the Contracting Authority, to determine, whether approved products shall be used, unless already defined by the NATO policies or equivalent national laws and regulations.

k. **Security Testing.** The system shall be subject to initial and periodic security testing to verify that security measures work as expected.

l. **Transmission Security.** NR information transmitted over a CIS not accredited to handle NR information (e.g. Internet) shall be encrypted using

approved cryptographic products.

m. **Wireless LAN:**

(1) The range of Access Points shall be set to minimise exposure to external attacks, special attention shall be given to the selection of antennae, their location, power and signal propagation.

(2) NR information transmitted over a wireless connection shall be encrypted using an approved cryptographic product.

n. **Virtualisation:**

(1) When existing systems are combined using a virtualisation product, the accreditation of each of the systems shall be reviewed to ensure that any mitigations and assumptions previously made are still appropriate.

(2) A deployed virtualisation product itself shall be treated as at least the highest Protective Marking of any of its virtual machines (i.e. NR).

(3) Virtual Machines shall be appropriately configured and managed. System patching, administration of accounts, and maintenance of anti-virus software, shall all be performed as if the machine were a physical machine. The host-operating machine shall also be correctly configured and maintained.

(4) Network routing provided internally by the virtualisation product to connect virtual machines shall not be considered as a security measure, e.g. a firewall shall not be virtualised.

(5) The administrative interface for the hypervisor, shall only be used for administration of the hypervisor, and shall not be used for the normal administration of services provided by the virtual machines.

(6) Access to the hypervisor functions shall be appropriately controlled.

(7) The ability to ‘cut-and-paste’ between virtual machines shall be appropriately configured and controlled.

(8) The ability to create virtual machines shall be appropriately configured and controlled.

(9) Virtual Machines shall be suitably de-commissioned after use.

(10) Software based virtual networks created between virtual machines shall be appropriately configured, controlled and monitored.

(11) Virtual Servers and Virtual Workstations shall not be located on the same physical host.

(12) Virtual machines operating in different areas of the system architecture shall not be located on the same physical host, for example, virtual machines operating in a De-Militarised Zone (DMZ) shall not be

located on the same physical host as those operating in the LAN.

(13) The management of the Virtualisation infrastructure shall be appropriately controlled. Only Virtual Management, patch management, anti-malware and Active Directory communication mode shall be allowed.

(14) Management of the Virtualisation infrastructure shall be performed via a dedicated Administrative Account.

(15) The Storage Area Network (SAN) used for Virtualisation shall be isolated and only accessible by the physical host.

(16) The SAN used to host Virtualisation operating at different security classifications shall be isolated onto Separate Logical Unit Numbers.

(17) Modifications to the 'Master Copy/Version' of a Virtual Machine shall be appropriately controlled.

(18) Network cards shall not be shared across Virtual Machines that are operating in different Security Domains.

o. **Interconnections to a CIS not accredited to handle NR information:**

(1) Security requirements, specific to interconnection scenarios, are listed in the latest versions of the NATO documents entitled "INFOSEC Technical and Implementation Directive for the Interconnection of Communications and Information Systems (CIS)" (current reference AC/322-D/0030-REV5) and "Supporting Document on the Interconnection of NR Communications and Information Systems (CIS) to the Internet" (current reference AC/322-D(2010)0058). These Directives may be obtained from the Contracting Authority.

(2) Interconnection to another CIS, especially the internet, 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. Security requirements can also be found in the latest version of the NATO document entitled "INFOSEC Technical & Implementation Directive for Computer and Local Area Network (LAN) Security" (current reference AC/322-D/0048-REV2). This Directive may be obtained from the Contracting Authority.

(3) When performed, the security risk assessment shall be included with the statement of compliance to the Contracting Authority.

p. **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 (SAA).

q. **Portable Computing Devices (laptops, tablets, etc.).** 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 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.

Physical Security of Communication and Information Services Handling NATO RESTRICTED information

27. 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.

28. 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.

Security of NATO RESTRICTED Removable Computer Storage Media

29. 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.

Use of Communication and Information Services Equipment Privately Owned by Contractor's Personnel

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

Communication and Information Services Users' Responsibilities

31. 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.

Advice

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

Audit/Inspection

33. 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.

ANNEX HH TO
AD 070-001
DATED 22 DEC 21

SECURITY ASPECTS LETTER (SAL)

1. In the performance of a contract, the prime Contractor and any Sub-contractor(s) are required to comply with NATO security regulations as implemented by the NSA/DSA of the nation in which the work is performed, or in the contracts involving NATO RESTRICTED (NR) information only as established in the Contract Security Clause.

2. All classified information and material shall be protected in accordance with the requirements established by the NSA/DSA of the nation in which the work is performed, or in the case of NR information, as may also be established in the Contract Security Clause.

3. In particular, the Contractor shall:

a. Appoint an officer to be responsible for supervising and directing security measures in relation to the Request for Proposals (RFP), contract or sub- contract;

b. 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 Personal Security Clearances (PSCs) at the required level where NC and above is involved;

c. Maintain, preferably through this officer responsible for security measures, 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 sub-contract is properly safeguarded;

d. Limit the copying of any classified materiel (including documents) to the absolute minimum to perform the contract;

e. Supply the NSA/DSA, when so requested by the latter, with any information on the persons who will be required to have access to NATO classified information;

f. Maintain a record of all employees taking part in 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;

g. Deny access to NATO classified information to any persons other than those authorised to have access by the NSA/DSA, or in the case of NR information, as determined by the need-to-know principle;

h. Limit the dissemination of NATO classified information to the smallest number of persons as is consistent with the proper execution of the contract or sub-contract;

i. Comply with any request that persons to be entrusted with NATO classified information sign a statement undertaking to safeguard that information and signifying their understanding of their obligations under national legislation on the safeguarding of classified information. Furthermore, that they recognise they may have comparable obligations under the laws of the other NATO nations in which they may have access to classified information;

j. Report to the Security Officer and to his NSA/DSA any breaches or