NCIA/ACQ/2020/6876

Acquisition Directorate
Boulevard Leopold III
B-1110 Brussels, Belgium

Telephone: +32 (0) 6544 6103

NCIA/ACQ/2020/6876
6 July 2020

To: All Nominated Prospective Bidders

From: The General Manager, NATO Communications and Information Agency (NCI Agency)

Subject: Request For Quotation (RFQ) No. RFQ-CO-115182-DAVS, Amendment No. 4, Answers to Clarification Requests

Provision for Discussion, Audio, and Video Systems (DAVS)

References:

A. AC/4-DS(2017)0020
B. Project Serial: 2016/2CM03999-M
C. NCIA/ACQ/2020/6774 RFQ-CO-115182-DAVS, dated 9 June 2020
D. NCIA/ACQ/2020/6808 RFQ-CO-115182-DAVS, Amendment 1 dated 16 June 2020
E. NCIA/ACQ/2020/6817 RFQ-CO-115182-DAVS, Amendment 2 dated 18 June 2020
F. F. NCIA/ACQ/2020/6850 RFQ-CO-115182-DAVS, Amendment 3 dated 29 June 2020

Dear Prospective Bidder:

1. At Reference C your firm was invited, in conformance with the terms of your active Basic Ordering Agreement (BOA) with the NCI Agency to participate in a BOA competition for the DAVS provision.
2. The purpose of this Amendment 4 to the RFQ is to publish the answers to the Clarification Requests (CRs) received to date for the subject RFQ. The answers provided does not require a revision to the RFQ. The Purchaser provided their response to the CRs attached as Annex A to this letter.
3. In accordance with the *Procedure Governing the Use of Basic Ordering Agreements concluded by the NATO Communications and Information Agency – 2019 version*", Ref: AC/4-D(2019)0004 (INV), Paragraph 30, the Book I, Part I, Bidding Instructions, Section 2, General Bidding Information, Paragraph 2.3.1, is hereby revised as follows:

FROM

"13:00 HOURS (BRUSSELS TIME) ON 9 JULY 2020

TO

13:00 HOURS (BRUSSELS TIME) ON 30 JULY 2020"

4. With the exception of the revisions mentioned above, all other RFQ documents remain unchanged from their original version as issued on 9 June 2020.

5. Prospective Bidder are advised that the NCI Agency reserves the right to cancel, withdraw, or suspend this RFQ at any time in its entirety and bears no liability for quotation preparation costs incurred by firms or any other collateral costs if RFQ cancellation, withdrawal, or suspension occurs.

6. The reference for the Request For Quotation is RFQ-CO-115182-DAVS, and all correspondence concerning this RFQ should reference this number.

7. The NCIA Agency sole point of contact (POC) for all information concerning this RFQ is Ms. Eva Benson, Contracting Officer, who may be reached at:

eva.benson@ncia.nato.int

FOR THE DIRECTOR OF ACQUISITION:

Eva Benson
Contracting Officer

Attachment:

(A) Purchaser answers to the Clarification Request
(B) Annex 1 Reference Document "*Technical and Implementation Directive on CIS Security*"

NCIA/ACQ/2020/6876

Distribution List for RFQ-CO-115182-DAVS

All Nominated Prospective Bidders	1 Each

NATO Delegations (Attn: Investment Committee Adviser):

Albania	1
Belgium	1
Bulgaria	1
Canada	1
Croatia	1
Czech Republic	1
Denmark	1
Estonia	1
France	1
Germany	1
Greece	1
Hungary	1
Iceland	1
Italy	1
Latvia	1
Lithuania	1
Luxembourg	1
The Netherlands	1
Norway	1
Poland	1
Portugal	1
Romania	1
Slovakia	1
Slovenia	1
Spain	1
Turkey	1

United Kingdom	1
United States	1
Belgian Ministry of Economic Affairs	1

Embassies in Brussels (Attn: Commercial Attaché):

Belgium	1
Bulgaria	1
Canada	1
Czech Republic	1
Denmark	1
Estonia	1
Germany	1
Greece	1
Hungary	1
Iceland	1
Italy	1
Latvia	1
Lithuania	1
Luxembourg	1
The Netherlands	1
Norway	1
Poland	1
Portugal	1
Romania	1
Slovakia	1
Slovenia	1
Spain	1
Turkey	1
United Kingdom	1
United States	1

NCI Agency - NATEXs

All NATEXs	1 Each

ANNEX E – Clarification Request Forms

RFQ-CO-115182 –DAVS

30 June 2020 and 3 July 2020

ADMINISTRATION or CONTRACTING					
Serial Nr	**RFQ Book**	**Art**	**QUESTION**	**ANSWER**	**Status**
A.1	All	All	Given the many description services requested and in order to fulfill NATO NCIA quality expectation, could we request NCIA procurement to have a supplementary delay of 3 weeks for the bid submission?	NCIA grants a three week Bid Closing Date extension from 9 July 2020 to 30 July 2020 at 1300.	Closed Amendment 4

RFQ-CO-115182 –DAVS

30 June 2020 and 3 July 2020

PRICE					
Serial Nr	**RFQ Book**	**RFQ Section Ref.**	**QUESTION**	**ANSWER**	**Status**
P.1	SSS sheet	Instruction Tab	*"Any changes in formula can be made at the bidder's discretions, as long as the detailed costs are clear, traceable and accurate as required. Ultimately the bidder is responsible for ALL values, formulas and calculations within the bidding sheets that are submitted to the Agency".* Question about this statement is when formula & inputs are changed, how can NCIA procurement made a comparison between different bidders with different totals, knowing that large excel sheet are difficult to control and that awarding criteria's are on the price only (with minimum technical compliancy)?	All costs within the CLIN Summary, Labour, Material, Travel and ODC sheets must be maintained at CLIN level and as per instruction provided in each sheet. Formulas can be adapted for flexibility but totals at CLIN level shall be consistent within the entire document. You are allowed to add sub-CLINs within the document, but always make sure you follow proposed CLIN structure to enable comparison at total CLIN levels.	Closed
P.2	SSS sheet	Several Tabs	Profit calculation is a yellow cell (example T2 in Tab labour) but this doesn't allow to have -as usual- individual product/service margin. Also, to increase clarity for NCIA purchase, we propose to put 0 in this cell and to fill in the specific NATO purchase price per items. Could you confirm this interpretation?	In case of individual product / service margin, please add extra yellow profit cell (e.g. cell U2, V2 etc.) and link it back with the relevant formulas in the profit column.	Closed
P.3	SSS sheet	Several Tabs	Several years (2020 to 2023) are mentioned in the sheet and need to be filled in (example in Tab Material). Because the project has a clear time frame (ex: + 44 weeks after contract date), many of the years will be empty and not sure (depending of contract award) that the cell with a content is on the correct year. Could you confirm the way to do this in the way that you expect?	Please maintain the prices in the year as accurately as possible as per your assumptions. In case you are not 100% sure please try the best you can to allocate the costs on the correct years.	Closed

P.4	SSS sheet	CLIN 8	In CLIN 8, there is no position for quoting services (Project management, installation and integration of Ops room, acceptance, training, etc…) Where can we integrate this services in the quotation file?	In order to quote for services, please use the bidding sheets labour, material, travel and ODC. For example if you want to add Project Management for CLIN 8, in the labour sheet, select the appropriate CLIN level (e.g. 8.1.1) and add project manager labour category and the rates as per instruction. In case of more than one labour category is required (e.g. installation and integration), you can add a new line for the same CLIN 8.1.1 and maintain another labour category with its specific rate (you can duplicate a CLIN line as many times as you need to reflect all the services associated to it).	Closed

RFQ-CO-115182 -DAVS

30 June 2020 and 3 July 2020

TECHNICAL					
Serial Nr	**RFQ Book**	**RFQ Section Ref.**	**QUESTION**	**ANSWER**	**Status**
T.1		1.2.2.26.	The Contractor shall install one (1) Amplifier in the Technical Booth of the JOC Floor Conference Room. Question: The listening room has only four speakers. Can we optimize the configuration by using the same amplifier as the JOC Floor conference room?	The intent to optimize the configuration is appreciated but NCIA shall stay with a dedicated, and same model amplifier for the listening rooms; therefore, this cannot be accepted.	Closed
T.2		1.2.2.9.1.1.2.	They shall be remotely powered (PoE) through Multi-Port Gigabit PoE Midspans, co-located with the Network Switches in the JOC Floor Conference Room Technical Booth; Question: Are we allow to power the encoder through powered chassis card instead of multiport Gigabit POE Midspans?	NCIA would not object if the bidder ensures that the powered chassis' are installed inside the custom cabinet underneath the Videowall. The chassis' would have to be vertically mounted to reduce the mounting depth and easy access must be guaranteed so cards can be hot-swapped if needed.	Closed

T.3		1.7.2.	On page 50, you state: *"The AV control systems have to meet the requirement defined at **Annex 1 to the reference 8.2.1.4"*** We are not able to find this annex you refer too. On Page 115 1.2.2.3. Core – AV Network you describe the following specifications for the switch. *1.2.2.3.1.1.6. Features:* *- At least a 1Gbps port per AVoIP Endpoint;* *- Non-blocking backplane;* *- IGMPv3 multicast snooping;* *- 802.1Q VLAN Tagging;* *- Port-Based 802.1P QOS;* *- 802.1X endpoint authentication;* *- Rapid Spanning Tree Protocol;* *- mDNS and DNS-SD;* *- Precision Time Protocol;* *- Energy Efficient Ethernet disabled;* *- The AVoIP network segment must receive network services, including DNS and DHCP;* *- Switches shall be stacked with support for multicast traffic;* *- Ethernet switch guidelines for AVoIP shall be implemented;* *- Ethernet switch guidelines for Dante shall be implemented.* What do we need to consider? (Important because Tempest specifications are missing here; what changes dramatically the budget).	NCIA corrects in Book II Part IV under Section 1.7.2 reference 8.2.1.4 to 9.2.1.4. Annex 1 is referenced only as stated in Section 9 of the SoW. This Annex was not provided, only referenced. Annex 1 is provided in this Amendment 4. NCIA would like to point out that the TEMPEST requirements were not missed; please view Section 1.7.5 of the SoW.	Closed Amendment 4

NATO UNCLASSIFIED
Releasable to North Macedonia

18 November 2019

DOCUMENT
AC/322-D/0048-REV3 (INV)

CONSULTATION, COMMAND AND CONTROL BOARD (C3B)

Technical and Implementation Directive on CIS Security

Note by the Secretary

Reference:

A. AC/322-WP(2019)0048-AS1 (INV), Request for C3B Approval of AC/322-D/0048-REV3: CIS Security Technical and Implementation Directive for CIS Security, 18 Nov 2019

1. On 18 November 2019, the C3 Board approved the Technical and Implementation Directive on CIS Security under a silence procedure, reference A. The document may be found at annex.

2. The releasability marking is used in support of the NATO member accession process and is not intended as a dissemination limitation marking. No additional approval of the originator is required to release this document outside of NATO for official NATO business.

3. Users of this directive are invited to submit suggested improvements to D/0048 to:

NS network: NHQC3SIACDBranch.Mailbox@hq.nato.int.
NU network: infosec@hq.nato.int.

4. This directive supersedes AC/322-D/0048-REV2, INFOSEC Technical Implementation Directive for Computer and Local Area Network (LAN) Security, 14 November 2011.

(Signed) S. NDAGIJIMANA-MUNEZERO

Annex 1: Technical and Implementation Directive for CIS Security

1 Annex

Action Officer: J. Boyd, 5478
Original: English

TECHNICAL AND IMPLEMENTATION DIRECTIVE FOR

CIS SECURITY

C3 Board Approval Date:

18 November 2019

PREFACE

A. This revision of D/0048 updates the directive to reflect changes to NATO security policy and evolution in technology. Beyond a normal periodic refresh, Revision 3 changes the scope of the directive from Computer and Local Area Network (LAN) security to Communication and Information System (CIS) security. Until recently, computing resources were situated and controlled within a single physical environment, with modest network connectivity. Today, restricting this directive to Computer and LAN security is no longer appropriate with the advent of cloud computing and network access methods able to support a mobile workforce.

B. Additionally, this revision shows the relationship of this document with the CIS Security Capability Breakdown and with PILAR, a Security Risk Assessment (SRA) tool commonly used by NATO. The CIS Security Capability Breakdown is a tool to report the maturity of NATO's CIS Security efforts to the C3 Board and other NATO Committees and Boards. Thus, the authors of this document have tried to avoid that D/0048 is an isolated document by tying it to the reporting framework and the SRA tool. This will improve the utility of this document.

Table of Contents

References 1-5
Introduction 1-7
Application of this Directive 1-8
Scope 1-8
PILAR 1-9
C3B Taxonomy 1-9
CIS Security Capability Breakdown 1-10
CIS Security Measures Organisation 1-11
CIS Protection: Endpoint Protection 1-12
Protection of Hardware and Media (PHM) 1-12
Protection of Software (PSW) 1-16
Protection of Services (POS) 1-19
Secure Maintenance (SMT) 1-25
CIS Protection: Network Protection and Boundary Protection 1-27
Network Security (NWS) 1-27
Control Systems (CS) 1-35
CIS Protection: Manage Personnel and Physical Security 1-39
Personnel Security (PS) 1-39
Physical and Environmental Security (PE) 1-43
CIS Protection: Data Protection 1-45
Data Protection (DA) 1-45
CIS Protection: Identity and Access Management 1-48
Identity and Access Management (IAM) 1-48
CIS Protection: Asset and Configuration Management 1-63
Configuration Management (CM) 1-63
Defend: Monitor and Detect, Audit 1-66
Logging, Continuous Monitoring and Audit (LMA) 1-66
Defend: Respond 1-73
Incident Response (IR) 1-73
Assess: Manage Risk and Plan Business Continuity 1-76
Continuity Planning (CP) 1-76
Sustain: Design and Implement, Manage Trustworthiness of CIS Components and Manage Supply Chain Security 1-78
Planning, Design and Implementation (PDI)
Sustain: Education, Train and Exercise 1-82
Security Education and Awareness (EA) 1-82

Glossary 1-84
Abbreviations and Acronyms 1-92

REFERENCES

A. C-M(2002)49, Security within the North Atlantic Treaty Organisation, 17 June 2002 (All corrigendum)
B. C-M(2002)60, The Management of Non-Classified Information, 11 July 2002
C. C-M(2007)0118, The NATO Information Management Policy, 11 December 2007
D. PO(2014)0358, Enhanced NATO Policy on Cyber Defence, 27 May 2014
E. PO(2014)0801, Minimum Requirements of CIS Security for National CIS Critical for NATO Core Tasks, 12 December 2014
F. AC/35-D/1037, Supporting Document for the Security of Electronic Registry Systems, 25 July 2006
G. AC/35-D/1039, Guidelines on Business Continuity Planning for Communications and Information Systems (CIS), 8 October 2008
H. AC/35-D/2000-REV7, Directive on Personnel Security, 7 January 2013
I. AC35-D/2001-REV2, Directive on Physical Security, 7 January 2008
J. AC/35-D/2002-REV4, Directive on the Security of Information, 17 January 2012
K. AC/35-D/2003-REV5, Directive on Classified Project and Industrial Security, 13 May 2015
L. AC/35-D/2004-REV3 Primary Directive on CIS Security, 15 November 2015
M. AC/35-D/2005-REV3 Management Directive on CIS Security, 12 October 2015
N. AC/35-N(2015)0022 (CISS), Rules of Engagement for Security Audits of NATO CIS, 20 October 2015
O. AC/322-D/0030-REV5 INFOSEC Technical and Implementation Directive for the Interconnection of Communications and Information Systems (CIS), 23 February 2011.
P. AC/322-D/0047-REV2, INFOSEC Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanisms, 11 March 2009
Q. AC/322-D/0049-REV1, INFOSEC Technical and Implementation Directive for Transmission Security, 29 November 2018
R. AC/322-D(2004)0030, INFOSEC Technical and Implementation Directive on the Requirement for, and the Selection, Approval and Implementation of, Security Tools, 17 May 2004
S. AC/322-D(2006)0041-REV2, Directive on the Selection and Procurement of NATO Common-Funded Cryptographic Systems, Products and Mechanisms, 21 Sep 2018
T. AC/322-D(2007)0036-REV2 (INV), INFOSEC Technical and Implementation Directive on Emission Security, 2 April 2019
U. AC/322-D(2007)0047, INFOSEC Technical and Implementation Supporting

Document on the Use of Shared Peripheral Switches, 12 September 2007

V. AC/322-N(2011)0130, Guidance on the Marking of NATO Information, 16 June 2011

W. AC/322-D(2012)0011, INFOSEC Technical and Implementation Directive on Downgrading, Declassification and Destruction of System Equipment and Storage Media, 7 June 2012

X. AC/322-D(2012)0012, INFOSEC Technical and Implementation Guidance on Downgrading, Declassification and Destruction of System Equipment and Storage Media, 7 June 2012

Y. AC/322-D(2015)0029, CIS Security Technical and Implementation Guidance on Protecting Authentication Credentials, 27 November 2015

Z. AC/322-D(2019)0034 (INV), C3 Taxonomy Baseline 3.1, 16 July 2019

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

BB. AC/322-D(2017)0044-REV1, CIS Security Technical and Implementation Directive on the Procurement and Use of Commercial PKI Certificates for Internet Facing NATO Websites, 18 January 2018

CC. AC/322-D(2018)0016, NATO Secure Voice Strategy, 14 March 2018

DD. AC/322-D(2019)0041 (INV), Technical and Implementation Directive on Introducing Secure Systems and Solutions Using Commercial Off the Shelf (COTS) Products Into NATO, 1 October 2019.

INTRODUCTION

1. Communications and Information System (CIS) Security is 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. Communication, Information and other electronic systems are referred to collectively as CIS in this directive.

2. This CIS Security directive is published by the C3 Board (C3B) in support of security requirements detailed in: Security within the North Atlantic Treaty Organisation (reference A); the NATO Information Management Policy (reference C); the Management of Non-Classified Information (reference B); the Enhanced NATO Policy on Cyber Defence (reference D); the Primary Directive on CIS Security (reference L) and is informed by the Minimum Requirements of CIS Security for National CIS Critical for NATO Core Tasks (reference E).

3. This directive supplements these policies by providing the minimum set of security measures required to be applied for the protection of NATO classified and non-classified information and the handling CIS. The description “NATO CIS” or “national CIS’ is used to denote who owns the CIS. As these security measures are based on a generic security risk assessment (SRA), the exact application of these measure for a particular CIS depends on the SRA maturity of the organisation. This is detailed below in *Application of This Directive*, **in particular paragraphs 6 and 7 whose understanding is essential in properly applying the security measures of this directive.** In any case, these security measures almost always will be augmented with other security measures based on the exact security requirements of a particular CIS.

4. These security measures shall be taken into consideration throughout the CIS life-cycle, as defined in the Primary Directive on CIS Security, reference L.

APPLICATION OF THIS DIRECTIVE

5. Entities owning and operating CIS handling NATO information have different Security Risk Assessment (SRA) maturity levels. Some entities will use the D/0048 baseline of security measures in lieu of a SRA, while other entities, like NATO, are required to perform a formal SRA for all their CIS. **To deal with the differing SRA maturity levels, *Mandatory* and *Recommended* are used in the following manner:**

6. Entities that do not perform a formal SRA on CIS:
   - SHALL implement *Mandatory* security measures.
   - SHALL implement *Recommended* security measures, unless they have Security Accreditation Authority (SAA) approval to deviate from them. Entities shall explicitly highlight mitigation measures to the SAA and these measures shall be approved by the SAA.

7. Entities that do perform a formal SRA on CIS:
   - SHALL implement *Mandatory* security measures. These entities may deviate from *Mandatory* security measures with prior SAA approval. Entities shall explicitly highlight mitigation measures to the SAA and these measures shall be approved by the SAA.
   - SHOULD implement *Recommended* security measures. At the least, they shall consider in their SRAs the risk which *Recommended* security measures mitigate.

SCOPE

8. Unless specifically identified, security measures shall be applicable for all security modes of operation as defined by the Primary Directive on CIS Security, reference L: “dedicated”, “system high”, “compartmented”, and “multi-level.” Those nations using multi-level security will have additional requirements beyond those found within this directive. When NATO has an approved multi-level security policy, this directive will be updated as required.

9. This directive shall be used by the NATO and National SAAs, CIS Planning and Implementation Authorities (CISPIA), CIS Providers (CISP), CIS Operational Authorities (CISOA), and Security Management Staffs responsible for establishing, implementing and operating NATO CIS or national CIS handling NATO information. In accordance with the Management Directive on CIS Security, reference M, the SAA for a particular CIS is responsible for checking the implementation of the security measures of this directive.

10. Where it states “for NATO CIS”, this directive is mandatory and binding upon CIS in NATO civil and military bodies. Where it states “for National CIS,” this directive is mandatory and binding upon national[1] CIS handling NATO classified information. As per reference B, paragraph 4, each nation shall use its best effort to keep NATO UNCLASSIFIED information from unauthorized disclosure. In consequence, nations should do their best efforts to respect *Mandatory* and *Recommended* security measures as per paragraphs 6 and 7 above for national CIS handling NATO UNCLASSIFIED information. This directive is mandatory and binding upon CIS handling both NATO classified and unclassified information for NATO related bodies, such as NATO Centres of Excellence (COEs) and Memorandum of Understanding (MoU) bodies, regardless of whether their CIS is provisioned by themselves, a nation or by NATO.

11. The requirements of the Directive on Cryptographic Security, reference P, and the Directive on the Selection and Procurement of NATO Commonly Funded Cryptographic Systems, Products and Mechanisms, reference S, specify the requirements for the use of cryptography. The requirements of the Directive on Emission Security, reference T, specify the requirements for emission security.

12. The security measures contained within this document are not applicable to Public Cloud solutions. Future policy is being developed by the C3 Board covering the security requirements of Public Cloud solutions.

PILAR

13. PILAR is a security risk assessment methodology tool recommended for NATO use by the NATO CIS Security Accreditation Board (NSAB). It is used by CIS Security architects and security accreditors within NATO. The authors have mapped D/0048 security measures with PILAR[2] measures to make this document more usable by NATO security architects, accreditors and other interested parties.

C3B TAXONOMY

14. The D/0048 Security Measures fall within the CIS Security Grouping of the C3B Taxonomy, reference Z. The CIS Security grouping overlaps with most levels (horizontal layers) of the C3 Taxonomy. As the C3 Taxonomy notes, the CIS Security Grouping should therefore not be seen as a level itself and rather as a logical grouping of critical components

[1] National: Includes national CIS of nations not members of NATO but which handle NATO information.
[2] Version 5.4

that jointly implement the tenets of CIS Security policies.

CIS SECURITY CAPABILITY BREAKDOWN

15. The CIS Security Capability Breakdown, depicted in Figure 1, below provides an overview of CIS Security capabilities. This C3B governance tool provides a framework of CIS Security Capabilities and their maturity levels. The security measures of D/0048 will be presented within this framework to facilitate NATO C3 governance.

16. Not all aspects of the CIS Security Capability breakdown are included within this document as some areas are already covered in existing policy and directives (such as the Cyber Defence policy) and are therefore not duplicated here (e.g. Inform is covered within Cyber Defence policy or Manage Risk is covered within reference M.).

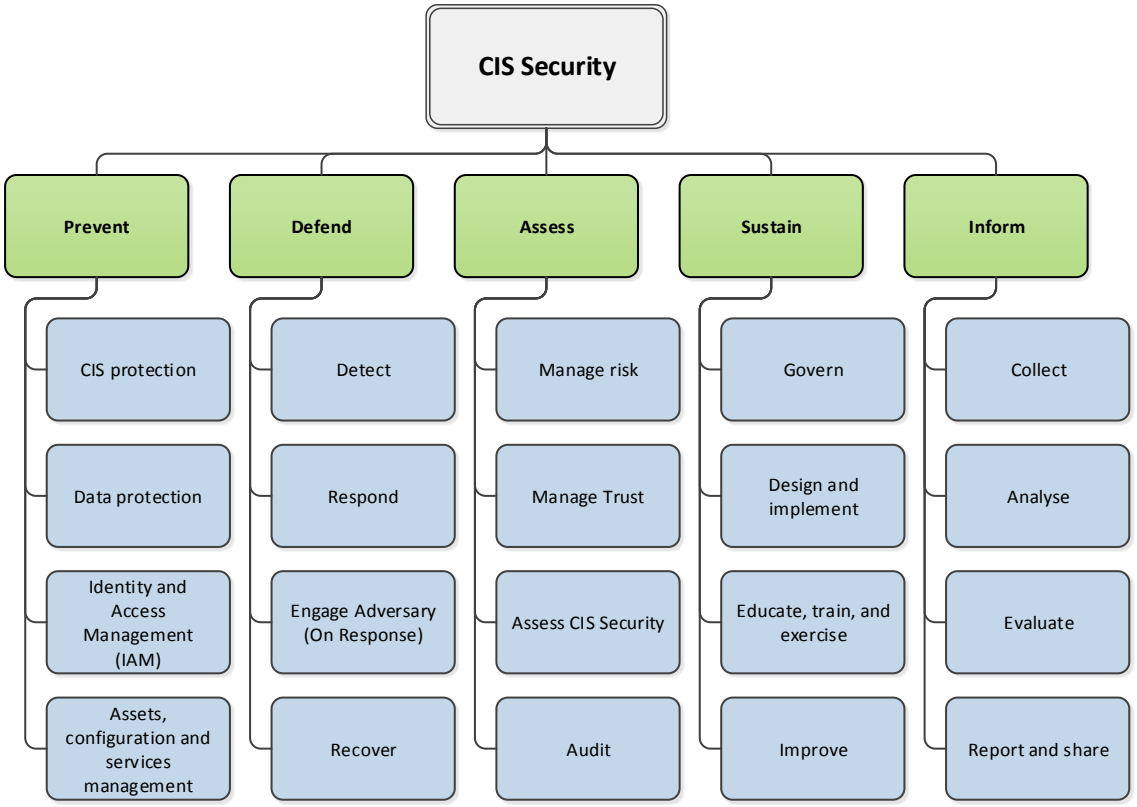

Figure 1 CIS Security Capability Breakdown

CIS SECURITY MEASURES ORGANISATION

17. The CIS Security measures of this Directive are organised into the following groups.

CIS Security Breakdown	D/0048 Security Measure Group
Section I: Prevent	
CIS Protection: Endpoint Protection	Protection of Hardware and Media (PHM)
	Protection of Software (PSW)
	Protection of Services (POS)
	Secure Maintenance (SMT)
CIS Protection: Network Protection; Boundary Protection	Network Security (NWS)
	Control Systems (CS)
CIS Protection: Manage Physical and Personnel Security	Personnel Security (PS)
	Physical and Environmental Security (PE)
CIS Protection: Data Protection	Data Protection (DA)
CIS Protection: Identity and Access Management	Identity and Access Management (IAM)
CIS Protection: Asset and Configuration Management	Configuration Management (CM)
Section II: Defend	
Monitor; Detect, Audit	Logging, Continuous Monitoring and Audit (LMA)
Respond	Incident Response (IR)
Section III: Assess	
Manage Risk and Plan Business Continuity	Contingency Planning (CP)
Section IV: Sustain	
Design and Implement; Manage Trustworthiness of CIS Components and Manage Supply Chain Security	Planning, Design and Implementation (PDI)
Education, Train and Exercise	Security Education and Awareness (EA)

Section I: PREVENT

CIS SECURITY BREAKDOWN CATEGORY: CIS PROTECTION, ENDPOINT PROTECTION

This Directive has four security measure groups in this category: Protection of Hardware and Media (PHM), Protection of Software (PSW), Protection of Services (POS), and Secure Maintenance (SMT).

D/0048 SECURITY MEASURE GROUP: PROTECTION OF HARDWARE AND MEDIA (PHM)

Protection of Hardware and Media security measures protect the tangible aspects of CIS Security – protection of the hardware and media processing or storing NATO information**.** Storage media includes, for example, diskettes, magnetic tapes, hard drives (including external/removable), SSD (Solid State Drive), USB (Universal Serial Bus) flash drives, compact discs, and digital video disks.

This section corresponds to the following PILAR elements: Protection of Hardware and Protection of Media.

ID	Security Measure **Protection of Hardware and Media**	NATO CIS		NATIONAL CIS Handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IMPORTANT: Read “Application of this Directive,” page 1-8, to understand the use of “M” and “R.”						
Section PHM1: Policy and Procedures						
PHM1-1	The CISP has documented Hardware and Media protection procedures.	M	M	R	R	
Section PHM2: BIOS/UEFI						
PHM2-1	BIOS/UEFI is accessible only by authorized privileged users.	M	M	M	M	If passwords are used, they shall be compliant with the requirements of section IAM4. See section IAM10 for privilege users’ access control restrictions.
PHM2-2	Security patching of BIOS/UEFI firmware is performed.	M	M	M	M	As per the requirements of PSW5-1, Security Patching and Updates.
PHM2-3	Unnecessary BIOS/UEFI features are disabled.	M	M	M	M	
PHM2-4	UEFI secure boot is enabled when available.	M	M	M	M	
Section PHM3: Emission Security (TEMPEST)						
PHM3-1	NATO Security policy requirements on Emission Security are implemented.	M	N/A	M	N/A	See reference T: Directive on Emission Security. Note: There are no TEMPEST restrictions on equipment processing NATO UNCLASSIFIED or NATO RESTRICTED information.
Section PHM4: Use of Shared Peripheral Switches						
PHM4-1	NATO policy requirements, or national equivalent, on shared peripheral switches are implemented.	M	M	M	M	See reference U: Supporting Document on Shared Peripheral Switches.

ID	Security Measure **Protection of Hardware and Media**	NATO CIS		NATIONAL CIS Handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
Section PHM5: Media Classification and Marking						
PHM5-1	CIS storage media is classified depending on the highest classification of data it is authorized to store.	M	M	M	M	This measure facilitates the proper handling of the storage media in order to protect the confidentiality of the contained information (e.g. to prevent the introduction of data above the allowed classification and to control the introduction of storage media from a higher classified CIS to a lower classified CIS unless explicitly allowed.)
PHM5-2	The maximum security classification (e.g. NS, NR), or protective marking (i.e. NU), of data that may be stored on a CIS storage media is identifiable.	M	M	M	M	For instance: the CIS storage media is labelled with the security classification or is labelled with a reference number, or the media serial number is used. This SM may be applied per storage media (e.g. USB drive) or group of media (e.g. SAN) as long as the intent below is met. Intent: to facilitate the proper handling of storage media to protect confidentiality and the proper decommissioning of storage media, as PHM8-1.
Section PHM6: Storage and Transport of Media						
PHM6-1	CIS storage media containing NS and above is registered as an accountable item by the relevant registry.	M	N/A	M	N/A	Where registration of embedded storage media is not possible or practical, the item with the embedded storage media shall be registered as an accountable item.
PHM6-2	In order to protect the integrity of the data and media and the confidentiality of the data, CIS storage media is physically transported in accordance with reference J and where appropriate, reference K.	M	R	M	R	Reference J: Directive on the Security of Information Reference K: Directive on Classified Project and Industrial Security SecOPs should detail the specific requirements.
Section PHM7: Removable CIS Storage Media Use						
PHM7-1	The use of removable CIS storage media requires authorization.	M	M	M	M	Both the number of authorized users and CIS media should be minimized to meet business requirements.

ID	Security Measure **Protection of Hardware and Media**	NATO CIS		NATIONAL CIS Handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
PHM7-2	Security measures prevent unauthorized removable CIS storage media being used on the CIS.	M	M	M	M	Security measures should be technical and not only procedural.
PHM7-3	The content of removable CIS storage media obtained from external CIS is checked for malware before it is made accessible to users or other services on a CIS for the first time.	M	M	M	M	Includes test and diagnostic media. Could be a system dedicated to the task of checking for malware, or the internal anti-malware software of the system which will use the removable storage media depending on local policy. Removable CIS from internal sources should be checked if there is reason to suspect the possibility of malware.
Section PHM8: Sanitization or Destruction of Media						
PHM8-1	CIS storage media which held NATO data will be sanitized or destroyed as per the requirements of reference W and the guidance of reference X, or national equivalent.	M	M	M	M	Includes SDD drives. Reference W: Directive on Downgrading, Declassification and Destruction of System Equipment and Storage. Reference X: Guidance on Downgrading, Declassification and Destruction of System Equipment and Storage Media

ANNEX 1
AC/322-D/0048-REV3 (INV)

D/0048 SECURITY MEASURE GROUP: PROTECTION OF SOFTWARE (PSW)

Protection of Software provides security measures for the protection of operating systems and applications.
This section corresponds to the following PILAR elements: Protection of Software

ID	Security Measure **Protection of Software**	NATO CIS		NATIONAL CIS Handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IMPORTANT: Read "Application of this Directive," page 1-8, to understand the use of "M" and "R."						
Section PSW1: Policy and Procedures						
PSW1-1	The CISP has documented Software protection procedures.	M	M	R	R	
Section PSW2: OS and Application Control						
PSW2-1	The authenticity and integrity of software and firmware are verified before installation.	M	M	M	M	Technical means (e.g. verifying signed software) are used when possible.
PSW2-2	The execution of applications is controlled in order to ensure authorized execution.	M	M	M	M	Applications include programs, Dynamic Link Libraries (DLL) and scripts. Examples of prevention strategies for unauthorized application execution include application whitelisting or code signing.
PSW2-3	The download or automatic execution of unauthorized mobile code is blocked.	M	M	M	M	Authorization of mobile code may be per code or per usage (e.g. Java Script on the Internet).
Section PSW3: Malicious Code and Anti-Malware						
PSW3-1	Protection against malicious code is deployed across the CIS in a multi-layer approach.	M	M	M	M	E.g. servers, endpoints (including handheld devices), web proxies, email guards and so on. Protection should include anti-virus; anti-spyware; anti-adware; anti-spam and anti-phishing etc. Embedded malware protection is authorized by the SAA or disabled.

ID	Security Measure **Protection of Software**	NATO CIS		NATIONAL CIS Handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
PSW3-2	Anti-malware diversity is used.	R	M	R	R	Different malware protection is used in the Boundary Protection Components (BPC) within the DMZ and internal network or different malware protection between servers and endpoints or both. Anti-malware diversity may include different engines or signature databases.
PSW3-3	The anti-malware solution uses more than signature based detection.	M	M	M	M	For instance uses heuristics, behavioural analysis, or static code analysis.
PSW3-4	Updates of the malware protection (e.g. signature definitions, heuristics) are deployed within 24 hours.	M	M	M	M	Deviation from this timeline is agreed with the SAA or the local CIS Security officer
Section PSW4: Application Security						
PSW4-1	Bespoke applications handling NATO information are developed following a defined Secure Software Development Life Cycle process which ensures security is taken into account during the design, development, testing, deployment, and operations phases of the application lifecycle.	M	M	M	M	
PSW4-2	Applications in scope of PSW4-1 are developed to employ data input and output sanitisation controls.	M	M	M	M	E.g. input sanitisation to prevent Cross Site Scripting (XSS), SQL injection, or buffer overflows.
PSW4-3	The CISP applies up to date hardening guidance to OS and configurable applications throughout their life-cycle.	M	M	M	M	E.g. NCI Agency or National CIS Security Authority (NCSA) hardening guidance. See Glossary for Software Hardening definition.

ID	Security Measure **Protection of Software**	NATO CIS		NATIONAL CIS Handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
PSW4-4	Operating Systems are approved by the SAA.	M	M	M	M	
PSW4-5	Application are security tested before the service is made available.	M	M	M	M	See CM3-4 for testing environment requirements.
PSW4-6	The testing environment assures the same level of security of the production environment if NATO production data (live data) is used during testing.	M	M	M	M	See CM3-4 for testing environment requirements.
Section PSW5: Security Patching and Upgrades						
PSW5-1	The CISP applies critical security patches within a week and non-critical security patches within four weeks.	M	M	M	M	Deviation are approved by the CISOA. (For example, delaying the application of a critical patch during a critical phase of an operation). Applicable to active VM templates as well.
PSW5-2	The organisation only uses versions of software that: • are supported with security patches; • do not require an obsolete version of OS, libraries and dependencies to function.	M	M	M	M	Exceptions shall be approved by the SAA.
PSW5-3	The CISP tests software and firmware updates before installation.	M	M	R	R	The CISP may skip testing for some critical security patches if they assess the risk of not testing is acceptable.
PSW5-4	The organization removes no longer required or unused software and firmware after updates.	M	M	R	R	

D/0048 SECURITY MEASURE GROUP: PROTECTION OF SERVICES (POS)

Protection of Services provides security measures for the protection of CIS elements which provide CIS support services.

This section corresponds to the following PILAR elements: Protection of Services and Protection of Hardware (for Virtual Machines).

ID	Security Measure **Protection of Services**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IMPORTANT: Read “Application of this Directive,” page 1-8, to understand the use of “M” and “R.”						
Section POS1: Policy and Procedures						
POS1-1	The CISP has documented services protection procedures.	M	M	R	R	
Section POS2: Virtualization Security						
POS2-1	All pertinent security measures in this document are applied to virtual machines (VM), in addition to the below controls specific to virtualization.	M	M	M	M	
POS2-2	The use of a Type 2 hypervisor shall be approved by the SAA and is only permitted on a specialised CIS, for a specifically authorised purpose, and with use and access technically limited to specifically authorised personnel.	M	M	M	M	Type 2 hypervisors could be used to bypass security measures, therefore use needs to be limited and controlled. Examples of suitable Type 2 hypervisors use cases include malware analysis, pen testing laptops, exercises, and test environments.

ID	Security Measure **Protection of Services**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
POS2-3	A physical server or server cluster only hosts VMs processing information of the same security domain.	M	M	M	M	The Intent is to prevent data leakage form one security domain to another using a VM escape. Reminder, the hosting of different security domains on a physical server or server cluster has to be approved by the SAA after a SRA.
POS2-4	The CISP controls VMs and containers throughout their lifecycle, from creation to deletion including maintaining of up to date configuration baselines.	M	M	M	R	See CM2-3 for VM template back-up requirements. Intent is to ensure VM templates are kept up to date with security patches and configurations and to ensure VM templates are used for their intended purposes. See PSW5-1 for patching timelines for active templates.
POS2-5	Users are able to utilize only authorized VM templates.	M	M	M	M	Users are constrained in which templates may be used.
POS2-6	VM's are made unavailable when not required.	M	M	M	M	E.g. suspend, shut down or terminate. Running a VM which isn't required provides no benefit but provides an additional attack surface.
POS2-7	Only authorized privileged users have the ability to create and modify VM templates.	M	M	M	M	
POS2-8	The unauthorised transfer of data between VMs, or between VMs and the user endpoint, is prevented by disabling access to endpoint shares from VMs.	M	M	M	M	E.g. clipboard or endpoint directory shares. The intent is to prevent the bypassing of security mechanisms enforced by the VM.
POS2-9	BPC are not hosted on the same physical server as the VMs they protect.	M	M	M	M	The intent is to prevent a BPC compromise by a VM escape from a compromised user VM. This SM does not apply to host-based BPCs (e.g. Windows Defender Firewall). See glossary for definition and examples of these interconnection protection components. See Section NWS2 for implementation of BPC/BPS.

ID	Security Measure **Protection of Services**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
POS2-10	Administration tools, if virtualized, are done so on dedicated physical servers.	M	M	M	M	
POS2-11	Bridging of network segments on a VM is authorized by SAA.	M	M	M	M	VM's of network functions (e.g. switching, routing, or firewall) are exempt.
Section POS3: Storage Area Networks						
POS3-1	All IP block storage security compliant implementations supports IPsec ESP to provide security for both control packets and data packets, as well as the replay protection mechanisms of IPsec. When ESP is utilized, per-packet data origin authentication, integrity and replay protection is used.	M	M	R	R	ESP=Encapsulating Security Payload
POS3-2	Fibre Channel SANs use hard zoning, port binding, port type control, WWN filtering and LUN masking.	M	M	M	M	WWN=Worldwide Name Number LUN=Logical Unit Number.
POS3-3	FC and IP SANs use mutual authentication.	M	M	M	M	FC= Fibre Channel, IP= Internet Protocol.
Section POS4: PKI Services						
POS4-1	PKI certificates are procured from a Certification Authority (CA) authorized by the appropriate PKI Policy Management Authority for the network.	M	M	M	M	For procuring commercial PKI certificates for NATO internet connected networks, see reference BB, Directive on the Procurement and Use of Commercial PKI Certificates for Internet Facing Websites.
POS4-2	The validity of PKI certificates are verified through all subordinate CAs to the Root CA.	M	M	M	M	

ID	Security Measure **Protection of Services**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
POS4-3	Cross-certification or mutual recognition (i.e. PKI Trust Lists) of another PKI requires NATO PKI Management Authority (NPMA) written approval.	M	M	N/A	N/A	
Section POS5: VoIP Security						
POS5-1	The use of VoIP technology on the CIS is authorized, controlled and monitored.	M	M	M	R	The CISOA is responsible for authorization, but may delegate the task to the CISP. The CISP controls and monitors. For NATO, use reference CC, NATO Secure Voice Strategy.
POS5-2	VoIP Devices authenticate to a VoIP server.	M	M	R	R	VoIP devices include IP phones as well as VoIP services integrated in other devices such as laptops, tablets or workstations.
POS5-3	IP Phones are secured like other network devices.	M	M	M	M	Unused services shall be shut down, unused ports disabled, and default management passwords changed. All management should be forced through authenticated and encrypted connections, if possible.
POS5-4	IP phones and VoIP servers are separated onto different networks from other CIS devices.	M	M	M	M	May be physically or logical (VLAN) separation. IP Phones and VoIP servers may be on different networks as well. IP Phones referred to are dedicated devices, not VoIP capability hosted in a computer, e.g. softphone such as Lync. The intent is separate IP phones and the VoIP server from other networked devices, thus reducing the attack surface, limiting unauthorized interception of calls and for QoS reasons.

ID	Security Measure **Protection of Services**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
POS5-5	VoIP protocols are protected between VoIP endpoints and servers.	M	M	M	M	E.g. SCIP (STANAG-5068, SCIP Minimum Implementation Profile module SCIP-221). Intent: to protect voice calls from targeted interception from the insider threat; or as part of the design of the security architecture to segment the CIS. Cryptography as per reference P, Directive on Cryptographic Security, for the protection of NATO classified and NATO UNCLASSIFIED information.
POS5-6	Interconnection between VoIP VLAN and mixed data VLAN is through a BPS.	M	M	M	M	For instance, to facilitate a call from an IP Phone to a VoIP service on a laptop while meeting the requirements of POS5-4. Intent is ensure that attacks from one VLAN is inhibited by the BPS from reaching the other VLAN For instance, it is essential that VOIP devices only are able to access servers in other VLANs required to set up and tear down phone calls (e.g. LDAP).
POS5-7	VoIP traffic leaving the security domain uses approved network encryption for confidentiality.	M	NR: M NU:R	M	NR: M NU:R	In accordance with reference P, Directive on Cryptographic Security, for the protection of NATO classified and NATO UNCLASSIFIED information.
Section POS6: Email Service Security						
POS6-1	Email spam, phishing and malware protection is provided at entry and exit points to the CIS (e.g. by using a secure email gateway).	R	M	R	M NOTE	Also known as Message Content Filtering. NOTE R for non-internet facing networks.
POS6-2	The CISP enables authenticity verification of outbound emails and uses protocols which facilitate the verification of inbound emails authenticity.	R	M NOTE	R	R	E.g. by using Domain-based Message Authentication, Reporting and Conformance (DMARC), Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) or similar technology. NOTE R for non-internet facing networks.

ID	Security Measure **Protection of Services**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
POS6-3	The use of a cryptographic protocol is enabled to provide confidentiality of email traffic between a Mail User Agent and a Mail Submission Server or Mail Access Server.	R	NU: M NR:R	R	R	The current RFC to provide this service is 8314, *Cleartext Considered Obsolete: Use of Transport Layer Security (TLS) for Email Submission and Access*. This capability is enabled so that it may be used if the distant end supports it as well. Some distant end organisations require the use of TLS for emails due to national privacy requirements (e.g. GDPR or HIPPA).
POS7: Internet Services Security						
POS7-1	Access to the Internet is via gateways which provide appropriate security services for the traffic they protect (e.g. anti-malware, browser exploit detection). The gateways are under the control of the CISP, unless otherwise authorised by the SAA.	M[NOTE] N/A CTS	M	M[NOTE] N/A CTS	M	[NOTE] NC/NS networks might be connected to the Internet via a one-way-diode importing data. POS7-1 gateway security services are mandatory for such connections. Access to the Internet is prohibited for CTS networks as per reference L, paragraph 7.12.6
POS7-2	Internet services proxy servers are used in conjunction with web blacklists and/or whitelists.	N/A	M	N/A	M	
POS7-3	Internet services proxy servers perform traffic analysis for all communication sessions, including encrypted sessions.	N/A	M	N/A	M	Includes Web Content Filtering. Traffic analysis for such things as malware and data leakage detection (DA3-1). E.g. encrypted sessions using TLS would be broken in a TLS proxy server in order to inspect packets
POS7-4	Web Application Firewalls (WAF) protect web applications.	R	M	R	M	WAF may also be used to protect internal web applications.
POS7-5	Internet facing websites or portals use TLS.	N/A	NR: N/A NU: M	N/A	NR: N/A NU: R	The intent, besides data confidentiality, is to mask traffic flows.

D/0048 SECURITY MEASURE GROUP: SECURE MAINTENANCE (SMT)

Maintenance performed in a manner which preserves the security of endpoints.
This section corresponds to the following PILAR elements: Protection of Software and Protection of Hardware.

ID	Security Measure **Secure Maintenance**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IMPORTANT: Read "Application of this Directive," page 1-8, to understand the use of "M" and "R."						
Section SMT1: Policy						
SMT1-1	The CISP implements documented Secure Maintenance procedures.	M	M	M	M	
Section SMT2: Controlled Maintenance						
SMT2-1	Technical security checks are performed after maintenance to verify proper secure functionality including TEMPEST.	M	M	M	R	May be performed by CISP, maintenance vendor or 3rd party. TEMPEST testing is performed when appropriate. Note: There are no TEMPEST restrictions on equipment processing NATO UNCLASSIFIED or NATO RESTRICTED information.
SMT2-2	Any type of maintenance is authorized and documented in accordance with configuration management procedures.	M	M	R[Note]	R	See Configuration Management section for documentation details. [NOTE] M for external maintenance.
SMT2-3	Only appropriately authorized or supervised personnel conduct maintenance.	M	M	M	R	See PS2-1 and associated note for the requirements for maintenance personal to be "authorized" Supervision is done by appropriately authorized CISP employee, as per PS2-1.

ID	Security Measure **Secure Maintenance**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
SMT2-4	If maintenance is conducted by a vendor on equipment containing classified information, the maintenance is conducted under the classified contract procedure as set out in reference K.	M	M	R	R	Reference K: Directive on Classified Project and Industrial Security.
SMT2-5	The confidentiality of data is ensured during maintenance.	M	M	M	M for NR	E.g. removal or sanitization of CIS storage media (see PM8-1); use of cleared maintenance personnel; use of data-at-rest encryption.
SMT2-6	The CISP restricts access to maintenance accounts and manages them as privilege accounts.	M	M	M	M	See IAM4-12 on default passwords and IAM8-3 for maintenance account requirements.
Section SMT3: Remote Maintenance						
SMT3-1	If remote maintenance is anticipated, it is explicitly authorized by the SAA during the accreditation process.	M	M	M	M	If remote maintenance is authorised the provisions of, Section NWS11, Remote Access, apply. See IAM8-3 and SMT2-6 for maintenance accounts requirements. The threats associated with the requirement for remote maintenance should be assessed for the requirement to implement additional security measures for controlling and monitoring.
Section SMT4: Organisational Data						
SMT4-1	The CISP ensures diagnostic files do not contain organisational data unauthorized for external maintenance entities.	M	M	M	R	Organisational data includes classified data, unclassified data with administrative markings (e.g. “Commercial” or “Staff”) or PII. It should be noted that some external maintenance entities may be authorised as per PS2-1 to handle some types of organisational data without sanitization (e.g. maintenance staff with security clearances) and this SM should be applied in a case by case situation.

CIS SECURITY BREAKDOWN CATEGORY: CIS PROTECTION, NETWORK PROTECTION and BOUNDARY PROTECTION

This Directive has two security measure groups in this category: Network Security and Control Systems.

D/0048 SECURITY MEASURE GROUP: NETWORK SECURITY (NWS)

Network security (NWS) encompasses both Network Protection and Boundary Protection. Network Protection includes the application of security measures, both in hardware and software, used to protect traffic sent between entities. This includes applications such as DNS services. Boundary protection limits the traffic flows between entities using various security measures such as filtering, blocking, termination, and redirection or otherwise modifying the flow. The purpose of Boundary Protection is to control access to resources and thereby preventing, stopping or mitigating attacks and faults. This section should be read in conjunction with reference O, AC/322-D/0030, the directive for the interconnection of CIS.

This section corresponds to the following PILAR elements: Protection of Communications, Protection of Services, and Interconnection Points: connecting to other trust zones.

ANNEX 1
AC/322-D/0048-REV3 (INV)

ID	Security Measure **Network Security**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IMPORTANT: Read “Application of this Directive,” page 1-8, to understand the use of “M” and “R.”						
Section NWS1: Network Design						
NWS1-1	The CIS network security design is approved by the SAA.	M	M	M	M	
NWS1-2	The CIS network security design fulfils the network security principles of references A and L.	M	M	M	M	E.g. availability, defence in depth, self-protecting CIS and resilience. Reference A: Security within NATO. Reference L: Primary Directive on CIS Security.
NWS1-3	At any time, the CISP is able to accurately determine in a timely manner network configuration including connections, flows and allowed services, protocols and ports.	M	M	M	M	
NWS1-4	Applications and Operating Systems are not configured as network appliances without SAA approval.	M	M	M	M	This does not prohibit software defined networking. Intent is to prevent uncontrolled network bridging or IP-forwarding by operating systems or applications. See POS2-11 for the VM use case.
Section NWS2: Boundary Protection Services						
NWS2-1	The CIS has Boundary protection services (BPS) at the interconnection to other CIS which provides at least IP packet filtering to secure the network and shield it from unauthorised data flows and users.	M	M	M	M	The BPS consists of components (BPC) which may be hardware and/or software (see glossary). Additionally, the BPS restricts unauthorised data from being exfiltrated out of the CIS.
NWS2-2	BPS are installed at key internal boundaries.	M	M	M	M	Internal BPS organises the network into multiple zones so that stateful inspection and policies can be applied for the traffic traversing these internal zones. E.g. the interconnection between server VLANs and other VLANs is a key internal boundary.

ID	Security Measure **Network Security**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
NWS2-3	For system components providing services which are accessible from another CIS, the CIS implements a DMZ to separate those components from other CIS components.	M	M	M	M	
NWS2-4	The CISP manages the number of external access points to minimize attack vectors whilst providing required availability.	M	M	M	M	
NWS2-5	Network services and information flows are allowed based on the “deny by default and allow by exception” principle.	M	M	M	M	
NWS2-6	The CIS routes external network web traffic through proxy servers.	M	M	R	R	
NWS2-7	The CIS detects and blocks outgoing traffic which may pose a threat to external CIS.	M	M	M	M	E.g. prevent routing of mal-formed packages, checking for malware, use of a private IP address in packets routed externally, DDoS attacks launched internally.
NWS2-8	The CIS monitors for the unauthorized exfiltration of data and implements preventive measures.	M	M	M	NR:M, NU:R	
NWS2-9	Boundary protection components are installed in a physically protected area, with access limited only to authorised CIS Security personnel/ privileged users.	M	M	M	M	See reference L, Primary Directive on CIS Security. See POS2-9 for VM requirements.

ID	Security Measure **Network Security**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
NWS2-10	BPCs are approved by the SAA.	M	M	M	M	
NWS2-11	Internal IP addresses are hidden from the Internet or similar networks in the public domain.	M	M	M	M	Network Address Translation (NAT) is a method of remapping one IP address space into another by modifying network address information in IP header of packets. NAT is generally used from NU/NR CIS to the Internet.
Section NWS3: BPC Management						
NWS3-1	The integrity of BPCs is protected during boot and operation.	M	M	M	M	
NWS3-2	Firewalls at interconnection boundaries fails safe, with no security downgrade, during a system failure.	M	M	M	M	
Section NWS4: Network Access Control						
NWS4-1	The CIS implements Network Access Control (NAC).	M	M	R	R	NAC provides the ability to dictate the activities that identified users and devices are able to use on the CIS (typically using IEEE 802.1X). This included the ability to enforce network restrictions based on policies and procedures. NAC may include Network Access Protection (NAP) and Network Access Quarantine (NAQ) services.
Section NWS5: Intrusion Detection and Prevention Services						
NWS5-1	The CIS implements network based Intrusion Prevention System (IPS) where possible, otherwise Intrusion Detection System (IDS) at external boundaries and key internal network segments.	M	M	M	M	As per the security architecture. At times an IPS is not appropriate, such as when there is a requirement of high throughput or the risk is unacceptable that false positives might automatically shut down a critical service.
NWS5-2	The organisation deploys host base IDS protection on critical system	M	M	M	M	For example, the traffic is encrypted at the network IDS.

ID	Security Measure **Network Security**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
	components whose traffic cannot be monitored by network IDS.					A Host-based Intrusion Detection System (HIDS) is a system that monitors a computer system on which it is installed to detect an intrusion and/or misuse, and responds by logging the activity and notifying the designated authority.
Section NWS6: Denial of Service (DOS) Protection						
NWS6-1	The CISP detects and protects against network Denial of Service (DoS) attacks.	M	M	R	R	The business and reputation impact of attacks guide the DoS prevention level of effort for a particular service.
Section NWS7: Transmission Security						
NWS7-1	When cryptography is used as a security measure to protect transmitted information, the requirements of reference P are met.	M	M	M	M	Reference P: Directive on Cryptographic Security. The C3B has approved the scope of reference P to also include NATO UNCLASSIFIED information as per the provisions of paragraph 1.
NWS7-2	Deployed CIS provides Traffic Flow Security (TFS) as per reference Q, when traffic flow analysis is identified as an unacceptable operational risk.	M	M	R	R	Reference Q: Directive for Transmission Security. Traffic-flow security is the use of various measures or methods to hide the presence of messages across a communicational medium, or to otherwise cloak messaging to prevent Traffic flow analysis and the observation of traffic levels across the CIS.
Section NWS8: Session Security						
NWS8-1	The CIS protects against session hijacking.	M	M	R	R	Session hijacking is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.
Section NWS9: Domain Name Services (DNS) and Name Resolution						
NWS9-1	Internal name/Address resolution services is from authoritative sources.	M	M	M	M	
NWS9-2	The CISP implements firewall rules for DNS security.	M	M	M	M	

ID	Security Measure **Network Security**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
NWS9-3	The CISP segregates internal and external DNS servers.	M	M	M	M	
NWS9-4	Forwarding DNS servers provides DNS services to internal DNS clients only.	M	M	M	M	
NWS9-5	The CISP restricts DNS zone transfers.	M	M	M	M	Physical segregation is preferred to logical segregation (e.g. BIND (Berkley Internet Name Domain) views concept.)
NWS9-6	The DNS service is not run as a privileged account.	M	M	M	M	
NWS9-7	Implement DNSSEC (Doman Name Security Extensions)	M	M	M	M	
NWS9-8	DNS-Zones re-signed with DNSSEC	M	M	M	M	
NWS9-9	DNS resolvers validates DNSSEC if used.	M	M	M	M	
Section NWS10: Wi-Fi Networks						
NWS10-1	The organization has only authorized Wi-Fi networks.	M	M	M	M	
NWS10-2	The organisation detects rogue Wi-Fi devices and access points and be capable of containing such devices.	M	M	M	R	This is normally done by the Wireless Intrusion Protection System (WIPS).
NWS10-3	Access to Wi-Fi networks containing organizational information uses IEEE 802.11, WPA2 encryption and EAP authentication.	M	M[NOTE]	M	M[NOTE]	NOTE: Encryption is recommended for access to Wi-Fi networks which only provide access to the Internet. Encryption in this case is as per reference P, Directive on Cryptographic Security. Or the latest encryption and authentication methods.

ID	Security Measure **Network Security**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
NWS10-4	The coverage of wireless access points is the minimal to fulfil business requirements.	M	M	M	M	
NWS10-5	Wi-Fi networking capability is disabled by default and is enabled only on authorized CIS components.	M	M	M	R	For NC and above, remove Wi-Fi drivers or hardware components for devices which do not require Wi-Fi capability ensuring activation, whether intentional or accidental, is impossible.
NWS10-6	Confidentiality of NATO classified information transmitted over Wi-Fi is protected with a NATO approved cryptographic mechanism as per reference P (e.g. with a VPN from device to Wi-Fi network).	M	M	M	M	Reference P: Directive on Cryptographic Security. The C3B has approved the scope of reference P to also include NATO UNCLASSIFIED information as per the provisions of paragraph 1.
NWS10-7	Users are not allowed to change network configuration in a way that would lower the security level.	M	M	M	M	For example, a user should only be allowed to modify wireless configuration if network exchanges are protected by a forced VPN tunnel configuration that is not user modifiable.
Section NWS11: Remote Access						
NWS11-1	All remote access is routed through managed access control points.	M	M	M	M	
NWS11-2	Use of approved encryption is required for any remote access to the CIS. Reference P is followed for encryption requirements.	M	M	M	M	Reference P: Directive on Cryptographic Security.
NWS11-3	If Remote access by privilege users is required, it is explicitly authorized by the SAA during the security accreditation process and strictly	M	M	M	M	

ID	Security Measure **Network Security**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
	controlled during the system operation.					
NWS11-4	The CISP is able to terminate remote access sessions and disable future remote access.	M	M	M	M	
NWS11-5	Split tunnelling for remote devices is not allowed.	M	M	M	M	
NWS11-6	Information exchange through the Internet is only allowed via remote access through the organisation's BPS.	N/A	M	N/A	M	Prevents direct access to the Internet for organisational owned devices. However organisationally owned devices (e.g. smartphone) which separate business and personal applications through approved functionality, direct access to the Internet by the personal sandbox is allowed.
NWS11-7	Access to Captive Portals is through approved applications which prevent further direct access to the Internet.	N/A	M	N/A	M	For instance, logging into a hotel's Wi-Fi through their Captive Portal is allowed, but then a VPN connection to the organisation's CIS must be immediately established. Note: There is a risk of a man-in-the-middle attack before the VPN is established.

D/0048 SECURITY MEASURE GROUP: CONTROL SYSTEMS (CS)

Control Systems (CS) deals with specific requirements for systems such as building management systems, audio-visual control systems or security control systems. Control systems may impact CIS Security in two ways. First, a CIS may host or serve as a bearer network for a control system, and this introduces additional vulnerabilities which must be controlled. This is a significant issue, as a control system may not have been designed with security in mind. Secondly, the security of the CIS may be dependent on a control system. For instance, the compromise of a physical security control system may allow unauthorized access to server rooms. Therefore, the below security measures apply when a control system is hosted or uses as a bearer network a CIS handling NATO information or when the control system provides security measures for a CIS handling NATO information.

This section corresponds to the following PILAR elements: Physical Access Control (in part)

ID	Security Measure **Control Systems**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IMPORTANT: Read “Application of this Directive,” page 1-8, to understand the use of “M” and “R.”						
Section CS1: General						
CS1-1	Control systems handling NATO information follow the security measures of this directive.	M	M	M	M	
CS1-2	The availability of the bearer CIS satisfies the availability requirements of the hosted control system.	M	M	N/A	N/A	

ID	Security Measure **Control Systems**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
CS1-3	Remote monitoring of control systems is approved by the SAA before implementation.	M	M	M	M	
CS1-4	Remote maintenance of control systems requires authorization by the SAA.	M	M	M	M	If remote maintenance is authorised, Section NWS11, Remote Access, apply. See IAM8-3 and SMT2-6 for maintenance accounts requirements. The threats associated with the requirement for remote maintenance should be assessed for the requirement to implement additional security measures for controlling and monitoring.
CS1-5	All remote connections to the control systems are identified, minimised and controlled.	M	M	M	M	
Section CS2: Physical Security Control Systems (PSCS)						
CS2-1	Physical separation or cryptographic separation is implemented between PSCS control systems and bearer CIS.	M	M	M	M	The security of the CIS relies on the physical security control system, which explains the more stringent requirements than for other control systems.
Section CS3: Other Control Systems						
CS3-1	Physical separation or cryptographic separation is implemented between control systems and bearer CIS which is not connected to the Internet.	M	R	M	R	For nations, M only applies to the confidentiality of NATO classified information.
CS3-2	Physical separation or cryptographic separation is implemented between control systems and bearer CIS which is connected to the Internet.	N/A	M	N/A	M	For nations, M only applies to the confidentiality of NATO classified information.

ID	Security Measure **Control Systems**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
CS3-3	The CISP, upon agreement with the SAA, physically or cryptographically separates different control systems from each other, depending on the control systems security needs.	M	M	M	M	For nations, M only applies to the confidentiality of NATO classified information.
Section CS4: Cryptographic Separation						
CS4-1	The Strength of Mechanism (SOM) required for cryptographic separation is based on the highest classification of the NATO information handled by either the control system or the CIS, as per reference P.	M	M	M	M	Reference P: Directive on Cryptographic Security.
Section CS5: Control System protocols						
CS5-1	SCADA and industrial protocols are only allowed within the control system network and not allowed to cross into the hosting CIS.	M	M	M	M	SCADA: Supervisory Control and Data Acquisition
Section CS6: Control System Management						
CS6-1	The SAA approves maintenance of a control system from the Internet, or similar networks in the public domain.	M	M	M	M	See SMT3-1 for remote maintenance requirements and Section NWS11 for remote access requirements.
CS6-2	Users accessing the control system from remote networks are required to authenticate using an appropriately strong mechanism.	M	M	M	M	E.g. token-based authentication.

ID	Security Measure **Control Systems**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
CS6-3	Computers and computerized devices used for control system functions (such as PLC programming) are not allowed to leave the control system area.	M	M	M	M	Laptops, portable engineering workstations and handhelds should be tightly secured and should never be allowed to be used outside the control system network. Antivirus and patch management should be kept current. PLC: Programmable Logic Controller
CS6-4	The use of unauthorized removable storage media on the control system is prevented.	M	M	M	M	In order to prevent the introduction of malware or the inadvertent loss or theft of data. E.g. CDs, DVDs, floppy disks, USB memory sticks.

CIS SECURITY BREAKDOWN CATEGORY: CIS PROTECTION: MANAGE PERSONNEL AND PHYSICAL SECURITY

This Directive has two security measure groups in this category: Personnel Security (PS) and Physical and Environmental Security (PE).

D/0048 SECURITY MEASURE GROUP: PERSONNEL SECURITY (PS)

This group covers the human element to CIS Security. Personnel security mitigates the risk to NATO information and associated CIS from untrustworthy personnel. CIS User is defined in the Glossary.

This section corresponds to the following PILAR elements: Personnel.

ID	Security Measure **Personnel Security**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IMPORTANT: Read “Application of this Directive,” page 1-8, to understand the use of “M” and “R.”						
Section PS1: Policy						
PS1-1	Personnel security measures are in accordance with reference H or national equivalent.	M	M for NR N/A for NU	M	M for NR N/A for NU	Reference H: Directive on Personnel Security. Reference H does not require a security clearance to access NR information, but does require a security awareness briefing on the obligation to protect NR information, see Section EA2 and EA3.

ID	Security Measure **Personnel Security**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
						Reference H does not specify requirements for NU information, however the education requirements of Section EA2 and EA3 apply.
Section PS2: Security Clearance						
PS2-1	All Individuals who may access NATO information classified NATO CONFIDENTIAL or higher have been granted the appropriate security clearance.	M	N/A	M	N/A	Note, as per reference L (Primary Directive on CIS Security), access to a CIS handling NATO information classified NATO CONFIDENTIAL or higher in dedicated, system high, or compartmented modes of operations is predicated upon an individual being cleared to the highest classification of information (NC and above) handled within the CIS. For CIS operating in the multi-level mode of operation, access to information classified NATO CONFIDENTIAL or higher is predicated on an individual being cleared to at least the classification of that information (NC and above) they are authorised to access. Note: Access to NR and NU information does not require a security clearance, however personnel accessing NR information have a security education briefing requirement, reference H Directive on Personnel Security. See reference H for the investigative requirements for NATO CONFIDENTIAL, NATO SECRET and COSMIC TOP SECRET security clearances for individuals who are: • Directly hired by a NATO civil or military body; • Seconded from a national governmental job to a position with a NATO civil or military body; • Individuals employed by a member nation and assigned to its national delegation at NATO HQ; • Or contactors working for NATO civil or military bodies. See SMT2-3 for maintenance personnel.

ANNEX 1
AC/322-D/0048-REV3 (INV)

<table>
<tr><th rowspan="2">ID</th><th rowspan="2">Security Measure
Personnel Security</th><th colspan="2">NATO CIS</th><th colspan="2">NATIONAL CIS handling NATO information</th><th rowspan="2">Remarks</th></tr>
<tr><th>NC/NS/CTS</th><th>NU/NR</th><th>NC/NS/CTS</th><th>NU/NR</th></tr>
<tr><td colspan="7">Section PS3: Privileged Users</td></tr>
<tr><td>PS3-1</td><td colspan="6">Remarks:
• The matrix below details the security clearance requirements by privilege Tier, highest level of classified information handled by the CIS, and whether NATO or national CIS.
• See Glossary for definition of Tier 0, Tier 1 and Tier 2 privileged users.
• The security clearance is a NATO or national equivalent. The required security clearance is a proxy for being trustworthy enough to assume a system administrator role at this level of responsibility. Background checks are as per PS2-1 and reference H, Directive on Personnel Security.
<table>
<tr><th rowspan="2"></th><th colspan="2">Tier 0 Privilege User</th><th colspan="2">Tier 1 Privilege User</th><th colspan="2">Tier 2 Privilege User</th></tr>
<tr><th>NATO</th><th>National CIS handling NATO Information</th><th>NATO</th><th>National CIS handling NATO Information</th><th>NATO</th><th>National CIS handling NATO Information</th></tr>
<tr><td>CTS</td><td>M: CTS</td><td>M: CTS</td><td>M:CTS</td><td>M:CTS</td><td>M:CTS</td><td>M:CTS</td></tr>
<tr><td>NS</td><td>M: CTS[1]</td><td>M: CTS[1]</td><td>M: NS</td><td>M:NS</td><td>M: NS</td><td>M: NS</td></tr>
<tr><td>NC</td><td>M:NS[1]</td><td>M:NS[1]</td><td>M:NS[1]</td><td>R:NS[1]</td><td>M:NC</td><td>M:NC</td></tr>
<tr><td>NR</td><td>M:NS[1]</td><td>M:NS[1]</td><td>M:NS[1]</td><td>R:NS[1]</td><td>M:NC[1]</td><td>M:NC[1]</td></tr>
<tr><td>NU</td><td>M:NS[1]</td><td>M:NS[1]</td><td>M:NS[1]</td><td>R:NS[1]</td><td>M:NC[1]</td><td>M:NC[1]</td></tr>
</table>
1. When the security clearance requirement for system administrators is greater than the classification or privilege marking (e.g. NU) of the CIS, then a privileged user may satisfy the requirement of PS3-1 with:
○ the specified NATO security clearance;
○ or national equivalent of the specified NATO security clearance;
○ or with a NATO or national security clearance equal to the classification of the CIS plus additional measures have been take to validate their trustworthiness to accept further responsibilities than a normal user. Reference H may be consulted for trustworthiness indicators and investigative requirements which would help fulfil this requirement.</td></tr>
</table>

ID	Security Measure **Personnel Security**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
	○ or with a NATO or national security clearance equal to the classification of the CIS and the activities of system administrators are constrained and monitored in a manner approved by the SAA. Monitoring of activities as per LMA2-1 and LMA7-2. Ways to constrain privilege users, to be formally confirmed by a security officer with comprehensive oversight, may include: ▪ they may not access unencrypted user data ▪ by default, they possess no administrator privileges and they are granted limited administrator privileges for a specific task and for a specific time frame ▪ critical administrator privileges are defined and two person approval is required to grant critical administrator privileges ▪ a security officer has comprehensive oversight demonstrable to the SAA					
PS3-2	Privileged users formally acknowledge the additional responsibilities due to their system administrative privileges.	M	M	M	M	

D/0048 SECURITY MEASURE GROUP: PHYSICAL AND ENVIRONMENTAL SECURITY (PE)

This group covers the ability to plan and control physical and environmental security supporting CIS Security. Physical and environmental security mitigates the risk to CIS components by threats from those vectors.

This section corresponds to the following PILAR elements: Protection of the Installations, Auxiliary means.

ID	Security Measure **Physical and Environmental Security**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IMPORTANT: Read “Application of this Directive,” page 1-8, to understand the use of “M” and “R.”						
Section PE1: Physical Security						
PE1-1	Areas where NATO classified information is stored or processed, and areas housing CIS supporting services, are compliant with reference I or national equivalent to reference I.	M	M for NR N/A for NU	M	M for NR N/A for NU	Reference I: Directive on Physical Security
PE1-2	Physical access is controlled to server rooms or data centres storing or processing NATO UNCLASSIFIED information.	N/A	M for NU N/A for NR	N/A	R	
PE1-3	Physical access is controlled to areas where unencrypted NATO classified information is in transit.	M	M for NR N/A for NU	M	M for NR N/A for NU	

ID	Security Measure **Physical and Environmental Security**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
PE1-4	Physical access is controlled to areas where CIS critical support services are hosted (e.g. power, light, air conditioning).	M	M	R	R	
PE1-5	Physical access to Tier 0 servers is limited to Tier 0 privilege users.	M	M	M	M	See SMT2-3 for maintenance personnel. See glossary for definition of Tier 0 privileged users.
Section PE2: Environmental security						
PE2-1	CIS critical components are protected from fire damage and appropriate fire prevention measures are taken.	M	M	R	R	
PE2-2	Critical CIS components are protected from water damage.	M	M	R	R	
PE2-3	Critical CIS components are provided with sufficient cooling.	M	M	R	R	
PE2-4	Critical CIS components are provided with adequate electrical power. (E.g. sufficient wattage, protection from power spikes).	M	M	R	R	

ANNEX 1
AC/322-D/0048-REV3 (INV)

CIS SECURITY BREAKDOWN CATEGORY: CIS PROTECTION: DATA PROTECTION

D/0048 SECURITY MEASURE GROUP: DATA PROTECTION

Data Protection covers the protection of data throughout its lifecycle and the assignment of security attributes to data (e.g. labelling) to assist protection.

This section corresponds to the following PILAR elements: Protection of Data/Information; Protection of Services: Personal data protection; Organisation: Personal data protection.

ID	Security Measure **Data Protection**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IMPORTANT: Read “Application of this Directive,” page 1-8, to understand the use of “M” and “R.”						
Section DA1: Data at Rest						
DA1-1	Outside of appropriate security area or administrative zone, the CIS cryptographically protects the confidentiality of “data at rest.”	M	M	M	R	For NC and above, this would be Class I or Class II security areas. See reference I, Directive on Physical Security, for the definition of the security areas and administrative zone. See PHM6-2 for physical protection of CIS storage media when transported outside of a secure area, e.g. to a different CIS.

ANNEX 1
AC/322-D/0048-REV3 (INV)

ID	Security Measure **Data Protection**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
DA1-2	The encryption mechanisms used for data at rest are compliant with reference P.	M	NR:M NU:R	M	NR:M NU:R	Reference P: Directive on Cryptographic Security.
Section DA2: Information markings						
DA2-1	Users assign and maintain human readable information markings during creation and modification of information as per references A and B.	M	M	M	M	Reference A: Security within NATO. Reference B: Management of Non-Classified Information. Information markings have four elements: Ownership, Classification, Releasability/Dissemination limitation and administrative/category, reference V, Guidance on the Marking of NATO Information.
DA2-2	A consistent interpretation of information markings are maintained during transmission between distributed CIS components.	M	M	M	M	See reference V, Guidance on the Marking of NATO Information, on information markings.
Section DA3: Audio and Video Capture						
DA3-1	Unapproved video or audio capture of NATO information is prevented.	M	M	M	NR: M NU: R	This may be implemented with technical means, or procedural means such as banning cell phones from an area, or controlling user behaviour in the SECOPs.
Section DA4: Data Loss Prevention						
DA4-1	Data loss prevention (DLP) measures are undertaken to detect and prevent potential data breaches at endpoints and during transmission.	M	M	M	M	DLP may be technical or procedural measures. See also POS7-3 for DLP at Internet boundaries.
Section DA5: Privacy						
DA5-1	Personally Identifiable Information (PII) is protected against unauthorised disclosure.	M	M	M	M	As per reference C, the NATO Information Management Policy. E.g. Compliance with the General Data Protection Regulation (GDPR) where applicable.

ID	Security Measure **Data Protection**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
DA5-2	The CISP notifies the CISOA when PII has been compromised.	M	M	M	M	As soon as the compromised has been suspected.

CIS SECURITY BREAKDOWN CATEGORY: CIS PROTECTION: IDENTITY AND ACCESS MANAGEMENT

D/0048 SECURITY MEASURE GROUP: IDENTITY AND ACCESS MANAGEMENT (IAM)

Effective identification and authentication measures counter the threat of an attacker authenticating as an authorized user to gain access to systems or data, and to have the ability to introduce unauthorized software or devices on the CIS. IAM also contain access control security measures that regulate users' access to information and manage users' and administrator rights (for example, read, write, modify, and delete).

Identification, Authentication, Access Control, CIS User and Remote Access are defined in the Glossary.

This section corresponds to the following PILAR elements: Identification and authentication, Logical Access Control.

ID	Security Measure **Identity and Access Management**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IMPORTANT: Read "Application of this Directive," page 1-8, to understand the use of "M" and "R."						
Section IAM1: Policy and Procedures						
IAM1-1	An Identity and Access Management policy which specifies the access control schema is developed.	M	M	M	M	
IAM1-2	User security attributes and access authorizations are defined.	M	M	M	M	
IAM1-3	Users read and acknowledge SecOPs, or national equivalent, prior to initial account use.	M	M	M	M	
Section IAM2: Identification						
IAM2-1	All users are identified, and their identity and attributes are managed throughout the users' lifecycle.	M	M	M	M	This may be done by a variety of parties: CISP, Security Office, Website Content Managers and so on.
Section IAM3: Authentication						
IAM3-1	User identity and possession of required privileges are confirmed during registration.	M	M	M	NR: M NU: R	This may be done by a variety of parties: CISP, Security Office, Website Content Managers and so on. CIS intended for public consumption (e.g. www.nato.int or public Wi-Fi) is exempted from identification requirement.
IAM3-2	Users are required to maintain authenticator confidentiality and are required to immediately inform the CISP or Security Officer of authenticator compromise, or suspected compromise.	M	M	M	M	Authenticator: A password, PIN or device (e.g. token, smartcard) used to authenticate to a CIS system.

ID	Security Measure **Identity and Access Management**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IAM3-3	The CISP disables authenticators that have been compromised or suspected of compromise.	M	M	M	M	Unless directed otherwise by the Incident Response Authority (as they may wish to observe attacker behaviour before an authenticator is disabled). See also IAM11-1 for automated lock of account.
IAM3-4	Users access CIS using multifactor authentication.	M	M	M	M	Includes VPN establishment from user devices (not applicable to TLS VPN connections to https websites for public access). Does not apply to non-enterprise users of publically accessible web portals/websites requiring authentication. See IAM12-3 and IAM12-4 for those requirements. SAA approves deviation from this requirement.
IAM3-5	The SAA is the sole authority which may authorize the use of shared accounts. If allowed, a procedure is established to maintain accountability.	M	M	M	NR: M NU: R	See Glossary for definition of shared account.
IAM3-6	Authenticator feedback information is obscured from the user during the authentication process.	M	M	M	M	E.g. password entry obscured with stars. No information should be displayed after failed attempt to indicate correct username.
IAM3-7	When authenticators for system and security administrator accounts are kept for emergency access, they are protected (e.g. sealed enveloped) in an appropriate security container.	M	M	M	M	

ANNEX 1
AC/322-D/0048-REV3 (INV)

ID	Security Measure **Identity and Access Management**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
Section IAM4: Password based Authentication[3]						
IAM4-1	The password composition policy requires users to choose a password at least 12 characters long while using a minimum of 3 of the 4 types of keyboard characters.	M	M	R	R	The SAA may approve variations if a system cannot accept a password of that length or a character set. This password policy was designed to balance password strength and usability. Keyboard character types: Upper case, lower case, number, and special character (e.g. %). For passwords used to administer or edit internet facing websites or portal, see IAM12-3.
IAM4-2	Commonly used passwords and substrings (e.g. “1234” or keyboard patterns) are banned by using password blacklists.	M	M	M	M	Sources for blacklist words may include for instance; • Passwords obtained from previous data breaches (e.g. Rockyou password database). • Dictionary words, in English, French and other NATO languages • Repetitive or sequential characters (e.g. ‘aaaaaaaa’ or ‘1234abcd’) • Keyboard patterns (e.g. ‘zaq12wsx’ or ‘qwertyuiop’) • Context specific words, such as names of NATO bodies or the username. The SAA or local security officer may allow deviance from this requirement if a system cannot use a password blacklist.
IAM4-3	Users do not re-use a password for a NATO account for any other account, whether NATO or non-NATO CIS.	M	M	M	M	This shall be stated in the SecOPs.

[3] When multi-factor authentication is not suitable. Includes memorized secrets and One Time Password (OTP) schemes.

ID	Security Measure **Identity and Access Management**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IAM4-4	Passwords are valid for between 1 to 3 years for CIS handling NC/NS/CTS information.	M	N/A	R	N/A	The password expiry period is agreed by the CISOA, CISP and SAA based on a balance of security, usability and cost. A password expiry floor is imposed as short password expiry periods provide an undesirable incentive for users to reuse passwords, choose weak passwords or write down passwords. Forced password expiration for reason of compromise is an exception (see IAM4-6).
IAM4-5	Passwords are valid for 1 to 2 years for CIS handling NU/NR information.	N/A	M	N/A	R	The password expiry period is agreed by the CISOA, CISP and SAA based on a balance of security, usability and cost. A password expiry floor is imposed as shorter password expiry periods provide an undesirable incentive for users to reuse passwords, choose weak passwords or write down passwords. Forced password expiration for reason of compromise is an exception (see IAM4-6).
IAM4-6	Password reuse is prohibited for 10 generations (i.e. users cannot re-use their last 10 passwords on a system).	M	M	R	R	E.g. the minimum password age limits the ability of users from cycling back to their old password. Or an alarm is raised if a user changes their passwords more than a certain number of times per month.
IAM4-7	Users have the ability to change their passwords in compliance with the requirements of IAM4-6.	M	M	M	M	The requirements of IAM4-1, IAM4-2 and IAM4-3 would apply to the new password.

ID	Security Measure **Identity and Access Management**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IAM4-8	The CIS stores only cryptographically protected passwords. Hashed passwords are salted with a unique and unpredictable salt per password.	M	M	M	M	The salt does not have to be a secret.
IAM4-9	The CISP only allows the use of temporary passwords for initial login and password reset. The CIS requires an immediate change of the temporary password to a permanent password. A temporary password has a short lifespan. A temporary password is for single use.	M	M	M	M	
IAM4-10	Password Managers, if utilized, are approved by the SAA.	M	M	M	M	Note that having a single Password Manager should be used for passwords from a single privileged user Tier (see Glossary for Tier definitions).
IAM4-11	The CISP changes default passwords on CIS (e.g. devices, service accounts, applications).	M	M	M	M	This passwords are then changed on a periodic basis, the timeframe depending on the password complexity and the criticality of the system and compliant with the requirements of IAM4-4 and IAM4-5.
IAM4-12	CIS components are not procured nor used with unchangeable passwords.	M	M	R	R	
IAM4-13	Passwords are handled at least at the same classification level of the CIS they protect. The storage of administrator passwords for emergency use is covered in IAM3-7.	M	M	M	M	See reference B, Management of Non-Classified Information, paragraph 18, on how to protect NU passwords.
IAM4-14	The use of One Time Passwords (OTP) is approved by the SAA	M	M	M	M	

ID	Security Measure **Identity and Access Management**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IAM4-15	The use of PINs in place of passwords are authorized by the SAA.	M	M	M	M	The intent is to facilitate secure authentication on devices where a password is not practical, such as smartphones, VOIP phones, printers and the like. The additional security risks of using a PIN should be understood and additional security measures considered to reduce those risks.
Section IAM5: PKI based Authentication[4]						
IAM5-1	PKI Authenticators are cryptographic devices and their approval is compliant with reference P or national equivalent.	M	M	M	M	Reference P: Directive on Cryptographic Security. PKI Authenticators may be in different formats: e.g. smartcards or USB PKI tokens.
IAM5-2	For PKI based authentication, the CISP ensures the CIS validates certificates by constructing and verifying a certificate path to a trust anchor including checking certificate status information.	M	M	M	M	
IAM5-3	The PIN or alphanumeric passcode used to access the PKI private key for logical access is not less than six digits or characters long.	M	M	M	R	
IAM5-4	The passcode (IAM5-3) is not easily guessed. The CISP enforces this if technically feasible.	M	M	M	M	

[4] Pertains to human authentication using a smartcard.

ID	Security Measure **Identity and Access Management**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IAM5-5	The smartcard is locked if the PIN or Passcode is incorrectly entered 5 to 10 times.	M	M	R	R	The exact number is agreed with the SAA.
IAM5-6	The CISP revokes PKI Certificates upon compromise or suspicion of compromise within the timelines specified in the Certificate Policy.	M	M	M	M	
IAM5-7	PKI Authenticators are dedicated to a security domain (i.e. a smartcard may not be used on both the NS and NU networks).	M	M	R	R	
IAM5-8	The CIS maintains a local cache of revocation data to support local path discovery and validation.	M	M	M	M	
IAM5-9	The CISP conducts the initial PKI registration process in-person (i.e. face-to-face) for human users or device sponsors.	M	M	M	M	Who may conduct the initial registration is detailed in the PKI Certificate Policy.
Section IAM6: Biometric Authentication						
IAM6-1	The use of biometrics is authorized by the SAA.	M	M	M	M	
IAM6-2	If a Mobile device uses biometrics, a password or PIN is entered initially and after a reboot.	M	M	M	M	

ID	Security Measure **Identity and Access Management**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
Section IAM7: Preventing Credential Theft and Reuse						
IAM7-1	The CISP prevents lateral movement of an attacker by using appropriate security measures.	M	M	M	M	For example: unique local account passwords, windows firewall rules, deny local accounts from having the privilege of performing network logons.
IAM7-2	The CISP hardens credential stores and mechanisms.	M	M	M	M	E.g. for Windows 10 Enterprise or Window Server 2016 use Microsoft Credential Guard. For service accounts, e.g. Microsoft Group Managed Service Accounts.
IAM7-3	Replay resistant authentication is required for access to user accounts.	M	M	M	M	A replay attack may enable an unauthorized user to gain access to the application. Authentication sessions between the authenticator and the application validating the user credentials must not be vulnerable to a replay attack. An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Techniques used to address this include protocols using a nonce (e.g. a number generated for a specific one-time use) or challenges (e.g., TLS, Web Services Security (WSS)). Additional techniques include time-synchronous or challenge-response one-time authenticators.
Section IAM8: Account Management						
IAM8-1	The CIS automatically logs account creation, modification, enabling; and privilege elevation, disabling and removal.	M	M	M	M	
IAM8-2	The CISP immediately disables CIS system access when no longer required (e.g. the termination of personnel employment; end of contract for contractor).	M	M	M	M	

ID	Security Measure **Identity and Access Management**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IAM8-3	Accounts used for maintenance are activated only for the period required and are subject to the privilege management requirements of section IAM10.	M	M	M	M	
IAM8-4	Inactive accounts are disabled within 90 days.	M	M	M	M	
IAM8-5	Unrequired accounts for deployed personnel are disabled from the date of deployment until user returns and reactivates account.	M	M	M	M	For deployments greater than 30 days.
IAM8-6	Service Accounts are tracked, disabled when no longer required and subject to the requirements of privilege user access controls.	M	M	M	M	See section IAM10 on privilege users' access control.
IAM8-7	Users protect CIS devices before leaving them unattended.	M	M	M	M	E.g. lock the operating system, physically secure the device.
Section IAM9: Access Control						
IAM9-1	User access to CIS and NATO information is controlled based on work requirements.	M	M	M	M	
IAM9-2	Security attributes are used by the system to determine access permissions.	M	M	M	M	
IAM9-3	Access profiles and their associated access rights are defined.	M	M	M	M	

ID	Security Measure **Identity and Access Management**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IAM9-4	The principle of Least Privilege applies: Users have the minimum set of permissions to accomplish their work tasks.	M	M	M	M	
IAM9-5	Normal users do not have local admin privileges (Tier 2) on their workstations.	M	M	M	M	See Glossary for the definition of Tier 2.
IAM9-6	User access permissions can be determined.	M	M	M	M	In other words, the CISP will be able to determine who has access to what resource.
IAM9-7	User access permissions are reviewed when a user changes roles.	M	M	M	M	Ensures least privilege and prevents privilege creep.
Section IAM10: Privilege Users Access Control						
IAM10-1	Administrator responsibilities are divided into three Tiers as per reference Y.	M	M	M	M	Reference Y: Guidance on Protecting Authentication Credentials. See Glossary for definitions of Tier 0, Tier 1 and Tier 2.
IAM10-2	Tier 0 and 1 administration and controlled maintenance is done only from computers dedicated to administration tasks of their respective tier, controlled by the organisation and without Internet or external CIS access.	M	M	M	M	See Glossary for definitions of Tier 0 and Tier 1 privileged users.

ID	Security Measure **Identity and Access Management**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IAM10-3	Tier 0 and 1 administration dedicated computers are hardened, only required software is installed and they are on a dedicated network segregated from the rest of the CIS with firewalls.	M	M	M	M	The dedicated network is made by either physical or logical means using an approved separation mechanism. Software permitting privilege escalation should be banished from Tier1 and Tier2 computers. Mechanism enforcing privileged users authentication policies are used (e.g. Protected Users, Authentication Silos…).
IAM10-4	Administration is not allowed from standard user accounts.	M	M	M	M	
IAM10-5	A privileged user working on several Tier have an account dedicated to each Tier and are only administrator of their administration computer when needed, not by default. Privileged users (i.e. administrators) use a non-privileged account when performing functions which do not require privileges.	M	M	M	M	It is possible that an administrator would have four accounts: Tier 0, Tier 1, Tier 2 and normal users. It is essential that the administrator only uses the account appropriate for the task at hand in order to prevent lateral movement or privilege escalation by an attacker who has managed to compromise a computer on the CIS.
IAM10-6	Administrator access to hypervisors is controlled.	M	M	M	M	If hypervisor hosts Tier 0 servers, then administrator access to this hypervisor is limited to Tier 0 privileged users (in accordance to POS2-7). The same restriction apply to resources used by this hypervisor. See Glossary for definitions of Tier 0.
IAM10-7	Privileged user's privileges are defined and current status can be determined.	M	M	M	M	

ID	Security Measure **Identity and Access Management**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IAM10-8	Privileges for privileged users are reviewed periodically and when an administrator changes roles.	M	M	M	M	Ensures least privilege and prevents privilege creep.
IAM10-9	Administrator privileges are managed to ensure least privilege.	M	M	M	M	
IAM10-10	The number of administrator privilege accounts is limited to the absolute minimum required.	M	M	M	M	
IAM10-11	The number of administrators with domain level privileges (Tier 0) is severely restricted.	M	M	M	M	Microsoft recommends only two Tier 0 account per Active Directory domain. See Glossary for definition of Tier 0.
IAM10-12	Only a subset of privileged accounts are explicitly authorized to access security functions.	M	M	M	M	Security functions might be log monitors or privilege management for example.
IAM10-13	Separation is maintained between internal security audit roles and access control management or privilege management roles.	M	M	R	R	
IAM10-14	Tier 0 and 1 administration computers system updates are not pushed from a lower Tier.	M	M	M	M	See section PSW5 for security patching and update measures. See Glossary for definition of Tier 0 and 1.

ID	Security Measure **Identity and Access Management**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
Section IAM11: Session Control						
IAM11-1	Session lock is implemented after a certain period of inactivity as agreed by the SAA; The requirement for CIS with exceptional operational requirements may be relaxed or omitted.	M	M	M	M	Examples of exceptional operational requirements might be a real time defence system or conference facilities.
IAM11-2	Concurrent sessions to a service by a single user are limited and monitored to prevent masquerading.	M	M	M	M	
IAM11-3	The CIS enforces a limit of unsuccessful login attempts after which at least one of the following measures is implemented: • the account is throttled; • the account or smartcard is locked; • the account is blocked for a predefined time; • the mobile device is purged/wiped.	M	M	M	M	Throttled: the access to the account is timed out for greater and greater period of time.
IAM11-4	The CIS displays system use notice information to the user before login is completed.	M	R	R	R	E.g. CIS classification, monitoring rules.

ID	Security Measure **Identity and Access Management**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
Section IAM12: Access to Internet-Facing Websites or Portals						
IAM12-1	Editors or administrators of publicly accessible websites or portals use multi-factor authentication, if available. If multi-factor authentication is not available, the passwords used are at least 16 characters long while using a minimum of 4 types of keyboard characters.	N/A	M	N/A	R	Keyboard characters: Upper case, lower case, number, and special character (e.g. %). Note IAM3-3, IAM4-2, IAM4-3, and IAM4-5 apply as well.
IAM12-2	Editors are designated, authorized and trained to publish publicly accessible information.	N/A	M	N/A	R	
IAM12-3	Passwords for users of publicly accessible websites, if used, meet the requirements of section IAM4, Password based Authentication.	N/A	M	N/A	R	
IAM12-4	The requirements for passwords of publicly accessible websites, when used in conjunction with another authentication factor, will be agreed by the SAA	M	M	M	M	Other Authentication methods: E.g. One Time Passwords (OTP), codes sent by SMS, or pre-distributed code lists. In conjunction with another authentication factor may include the code concatenated with the password; or a two-step authentication processing using another authentication factor then a password or vice versa. The requirements of passwords or PINS used to activate multi-factor authentication devices such as smartcards are detailed in IAM5-3.

CIS SECURITY BREAKDOWN CATEGORY: CIS PROTECTION: ASSET AND CONFIGURATION MANAGEMENT

D/0048 SECURITY MEASURE GROUP: CONFIGURATION MANAGEMENT

Configuration management establishes and maintains the security of CIS through the maintenance of accurate inventories and through control of processes for initializing, changing, and monitoring the configuration of CIS throughout the system development lifecycle.

This section corresponds to the following PILAR elements: Protection of Services: Change Management and Change Management Control; Protection of Software: Changes (updates & maintenance); Protection of Hardware: Changes (updates & maintenance); Protection of Communications: Changes (updates & maintenance);

ID	Security Measure **Configuration Management**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IMPORTANT: Read “Application of this Directive,” page 1-8, to understand the use of “M” and “R.”						
Section CM1: Policy and Procedures						
CM1-1	The CISP has documented Configuration Management procedures including handling of emergency changes.	M	M	M	M	

ID	Security Measure **Configuration Management**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
Section CM2: Component Inventory						
CM2-1	An accurate inventory(s) of CIS hardware and software is maintained.	M	M	M	M	
CM2-2	The CISP, the SAA, or both, develops and maintains in a coordinated manner baseline configurations of CIS components.	M	M	R	R	As per agreement with the SAA. Includes VM templates (POS2-4).
CM2-3	At least the previous baseline configuration is maintained for each CIS component.	M	M	R	R	More may be maintained if required.
Section CM3: Configuration Change Control						
CM3-1	A configuration change control process validates, tests, documents and approves all changes to the CIS. This includes a security impact analysis performed by security experts for all changes to the CIS baseline.	M	M	M	M	
CM3-2	New or modified versions of software are checked for integrity and for malware before being introduced to the CIS.	M	M	M	R	
CM3-3	New or modified versions of equipment are validated prior to their introduction in the system.	M	M	R	R	Validation could include: compatibility with existing CIS, proper secure configuration, conformance to the security baseline, physical integrity.
CM3-4	A separate test environment is used to assess new or changed capabilities	M	M	R	R	Capabilities include applications and hardware.

ID	Security Measure **Configuration Management**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
	before introducing them to the operational CIS.					
Section CM4: Access Restriction for Change						
CM4-1	Only authorized privileged users implement changes to the CIS baseline.	M	M	M	M	
CM4-2	Configuration changes to the CIS are audited.	M	M	M	M	
Section CM5: Configuration Settings						
CM5-1	Configuration settings are established, documented and approved for components employed in the CIS.	M	M	M	M	I.e. hardware, software, VMs etc.
CM5-2	Components within the CIS are configured to provide only required capabilities (least functionality). Components which are not required are either uninstalled, not installed or disabled.	M	M	M	M	
CM5-3	The configurations of components within the CIS are periodically verified against the approved baseline.	M	M	M	M	

SECTION II: DEFEND

CIS SECURITY BREAKDOWN CATEGORY: DEFEND: MONITOR and DETECT, AUDIT

D/0048 SECURITY MEASURE GROUP: LOGGING, CONTINUOUS MONITORING AND AUDIT

Logging and Continuous Monitoring provide a means to provide sufficient information to be able to investigate a deliberate, accidental or attempted compromise of the security objectives for NATO CIS and information and the ability assess the damage arising from any compromise. Regular audits help maintain continuous awareness of CIS Security, vulnerabilities and threats. This is distinct from a security audit, which is a SAA formal periodic systematic review of a CIS to ascertain its susceptibility to compromise. The requirements of security audits are detailed in reference L, the Management Directive on CIS Security.

See Glossary for definitions of Logging, Continuous Monitoring and Audit.

This section corresponds to the following PILAR elements: Logging and Audit, and Security Tools.

ID	Security Measure **Logging, Continuous Monitoring and Audit**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IMPORTANT: Read “Application of this Directive,” page 1-8, to understand the use of “M” and “R.”						
Section LMA1: Policy and Procedures						
LMA1-1	The organisation has a documented and Logging, Continuous Monitoring and Audit procedures.	M	M	M	R	See reference N for the rules of engagement for security audits.
Section LMA2: Logging						
LMA2-1	The OS and hypervisor logs contain, as a minimum: • authentication events; • File and object events; • export (e.g. upload) and import (e.g. download) events; • user account events; • privilege user events.	M	M	M	M	User account events are detailed in IAM8-1.
LMA2-2	The CISP/CISPIA, in conjunction with the SAA and CISOA, identify any additional logging requirements in order to support the detection and investigation of security incidents affecting the CIS.	M	M	M	M	Any additional logging requirements are documented in the security accreditation documentation. The additional logging needs of all the CIS is considered, including its infrastructure, network, supporting services, operating systems and applications.

ID	Security Measure **Logging, Continuous Monitoring and Audit**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
LMA2-3	Log records contain as a minimum: • timestamp; • event, status and/or error codes; • service/command/application; • name/user(s) or system account(s)associated with an event; • device used (e.g. MAC address, source and destination IP address, web browser.)	M	M	M	M	
LMA2-4	Aggregated and correlated review and analysis of logging records are possible.	M	M	M	R	Preferred method is the real time transfer of logs from the original machine to the log repository.
Section LMA3: Time Stamps						
LMA3-1	An authoritative time source is used.	M	M	M	M	The intent is for time stamps on logs to be derived from the same authoritative time source in order to facilitate digital forensics. Synchronisation may be achieved through the use of protocols such as Network Time Protocol, NTP, or Precision Time Protocol (PTP) and the like, which are designed to synchronize system clocks over a network to an authoritative time source.
Section LMA4: Response to Logging Collection Failure						
LMA4-1	The CIS provides an alert in response to logging collection failures.	M	M	M	M	
LMA4-2	The CIS provides an alert before logging storage capacity is exceeded.	M	M	M	M	Recommended that an alert triggers when logging storage capacity reaches 75%.

ID	Security Measure **Logging, Continuous Monitoring and Audit**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
Section LMA5: Protection of Log Information						
LMA5-1	Logs are protected from unauthorized access modification and deletion.	M	M	M	M	
LMA5-2	Logs are classified and protected at the same level as the classification of the information they contain.	M	M	M	M	
Section LMA6: Logging Record Retention						
LMA6-1	Logging records for access to NATO information are kept either online or offline for: CTS CIS 10 Years NS CIS 5 Years NC/NR/NU CIS 3 Years	M	M	R	R	For example: SharePoint server, file share. Record do not have to be online for this whole period, but must be available in a reasonable time to facilitate possible future investigations. The retention period is informed by relevant NATO or national policies. Pertinent NATO policy includes: • Reference F: Supporting document on the Security of Electronic Registries. Reference F requires logs for access to NS information in a registry to be kept for at least 5 years after its destruction • Reference J, Directive on the Security of Information. Reference J requires logs for access to CTS information in a registry to be kept for 10 years after its destruction. Reference J does not require access to NC, NR and NU information to be accountable, however it is still essential to review logs to determine method of compromise.
LMA6-2	Logging records of other network components are kept for an agreed period of time. The period is agreed by CISP and the SAA.	M	M	M	M	Enables possible future investigations.

ID	Security Measure **Logging, Continuous Monitoring and Audit**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
LMA6-3	The CIS has sufficient storage capacity (online supplemented by an offline archive) to meet the requirements of LMA6-1 without the risk of over-writing required logging records.	M	M	M	M	
LMA6-4	Offline archived logging records are not assessable from the CIS being logged.	M	R	R	R	
Section LMA7: Continuous Monitoring						
LMA7-1	The CIS and its interconnection(s) are automatically and continuously monitored to detect abnormalities, attacks and unauthorised use.	M	M	M	M	
LMA7-2	Privilege users are continuously monitored for misuse or abnormal use of privileges.	M	M	M	M	
LMA7-3	The CIS is continually assessed for vulnerabilities.	M	M	R	R	
LMA7-4	The threat against the CIS is continually assessed.	M	M	M	M	
LMA7-5	Continuous monitoring systems automatically generate security alarms to notify security staff.	M	M	M	M	
LMA7-6	Continuous monitoring systems have the ability to automatically assign criticalities to security alarms.	M	M	R	R	

ID	Security Measure **Logging, Continuous Monitoring and Audit**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
Section LMA8: Log Review						
LMA8-1	Log review, analysis and reporting is performed on a periodic basis in order to detect security issues and unusual trends.	M	M	M	R	Automated tools are preferred. Periodic basis is agreed per system by CISP and SAA.
LMA8-2	Log review analysis and reporting is correlated with activities such as monitoring, scanning, incident response or other sources.	M	M	R	R	Other sources can include list of stolen devices, etc.
Section LMA9: Use of Security Tools (ST's)						
LMA9-1	Only formally authorised personnel use Security Tools.	M	M	M	M	Personnel e.g. CERT staff, Vulnerability Assessment Team Tools e.g. network scanners, password crackers.
LMA9-2	Unauthorized access to security tools is prevented.	M	M	M	M	
LMA9-3	The Security Tool successfully pass an assessment process by a recognized NATO or National body (E.g. SECAN, NCI Agency, or a NCSA). Or security tools are selected from the NATO IA Product Catalogue (NIAPC); or have subject to a Security Test and Evaluation plan agreed by the SAA.	M	M	R	R	See reference R: Directive on the Requirement for, and the Selection, Approval and Implementation of, Security Tools.
LMA9-4	The use of Security Tools is in accordance with reference R.	M	M	R	R	Reference R: Directive on the Requirement for, and the Selection, Approval and Implementation of, Security Tools.

ID	Security Measure **Logging, Continuous Monitoring and Audit**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
LMA9-5	The CISP identifies and mitigates vulnerabilities arising from the use of the Security Tool.	M	M	M	M	

CIS SECURITY BREAKDOWN CATEGORY: DEFEND: RESPOND

D/0048 SECURITY MEASURE GROUP: INCIDENT RESPONSE

Incident Response is the ability to handle CIS Security incidents, including personnel, equipment, plans and procedures.

This section corresponds to the following PILAR elements: Incident management.

ID	Security Measure **Incident Response**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IMPORTANT: Read “Application of this Directive,” page 1-8, to understand the use of “M” and “R.”						
Section IR1: Policy and Procedures						
IR1-1	The CISP has a documented CIS Security Incident Response procedures.	M	M	R	R	Includes notification requirements.
IR1-2	CIS Security Incident Response procedures ensures the preservation of data for evidence purposes according to forensics best practices.	M	M	M	M	

ID	Security Measure **Incident Response**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
Section IR2: Capability						
IR2-1	The CISP has a CIS Security incident response capability responsible for the local level (at least a CIS Security Officer).	M	M	M	M	
IR2-2	The CISP has the capability to provide additional support to local CIS Security incident response.	M	M	M	M	
IR2-3	The CISP has the capability to coordinate CIS Security incidents organisation wide and coordinate incident response with outside organisations.	M	M	M	M	
Section IR3: Recovery						
IR3-1	The CISP has the capability to contain an attack, restore systems, data and connectivity in a prioritized manner.	M	M	R	R	
Section IR4: Inform						
IR4-1	The CISP reports CIS Security incidents affecting the CIS as required by reference L.	M	M	M	M	Reference L: Management Directive on CIS Security.
Section IR5: Lessons Identified, Feedback and Testing						
IR5-1	The CISP identifies, communicates and builds upon lessons learned.	M	M	R	R	
IR5-2	After incidents, the CISP implements lessons identified.	M	M	R	R	E.g. Updates key information, controls and processes.

ID	Security Measure **Incident Response**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IR5-3	The CISP performs CIS Security incident trend analysis to improve its CIS Security posture and ability to respond to incidents.	M	M	R	R	
IR5-4	The CISP periodically tests its security incident plans and procedures.	M	M	M	M	

SECTION III: ASSESS

CIS SECURITY BREAKDOWN CATEGORY: ASSESS: MANAGE RISK and PLAN BUSINESS CONTINUITY

D/0048 SECURITY MEASURE GROUP: CONTINUITY PLANNING

Continuity planning is required to mitigate interruption of service due to CIS Security incidents. Continuity planning for CIS Security incidents is part of business continuity planning. Reference G, Guidelines on Business Continuity Plans for CIS, provides more detail and background information.

This section corresponds to the following PILAR elements: Business continuity (contingency).

ID	Security Measure **Continuity Planning**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IMPORTANT: Read “Application of this Directive,” page 1-8, to understand the use of “M” and “R.”						
Section CP1: Policy and Procedures						
CP1-1	The organisation has a documented Continuity Planning procedure.	M	M	R	R	
CP1-2	The organisation has a CIS continuity plan and reviews it regularly.	M	M	R	R	

ID	Security Measure **Continuity Planning**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
CP1-3	The CIS continuity plan is integrated with the organisation's business continuity plan.	M	M	R	R	
CP1-4	The organisation tests the effectiveness of the CIS continuity plan at least annually.	M	M	R	R	
Section CP2: Failover/Load Balancing						
CP2-1	The CIS implements automatic failover/load balancing for critical CIS components.	M	M	R	R	
Section CP3: Back Up						
CP3-1	The organisation establishes a strategy for back-up, including data, logs, software, baseline configuration and VM templates.	M	M	R	R	
CP3-2	The back-up and restoration process is tested as frequent as required by the CISOA. The test plan is documented and provided to the SAA.	M	M	R	R	
CP3-3	Data back-ups are stored so that an incident cannot impact both the CIS and its back-ups.	M	M	R	R	

SECTION IV: SUSTAIN

CIS SECURITY BREAKDOWN CATEGORY: DESIGN AND IMPLEMENT, MANAGE TRUSTWORTHINESS OF CIS COMPONENTS and MANAGE SUPPLY CHAIN SECURITY

The below D/0048 Security Measure group has aspects in two CIS Security Breakdown Categories. Part is in Sustain: Design and Implement to ensure proper design of CIS Security. The other part is in Assess: Manage Trustworthiness of CIS Components and Manage Supply Chain security which aims to ensure the acquisition of trustworthy hardware.

D/0048 SECURITY MEASURE GROUP: PLANNING, DESIGN AND IMPLEMENTATION

This group details measures for the proper planning and design of CIS Security, the acquisition of trustworthy hardware and software and their secure implementation.

This section corresponds to the following PILAR elements: Acquisition/development

ANNEX 1
AC/322-D/0048-REV3 (INV)

ID	Security Measure **Planning, Design and Implementation**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IMPORTANT: Read “Application of this Directive,” page 1-8, to understand the use of “M” and “R.”						
Section PDI1: Policy and Procedures						
PDI1-1	The CISP and CISPIA implements documented CIS Planning procedures and CIS system and service acquisition procedures.	M	M	R	R	E.g. align with reference architectures; outsourcing design documentation requirements concept of operations; security goals and objectives.
PDI1-2	The security aspects of acquisition policies are followed.	M	M	R	R	
PDI1-3	The organisation develops and enforces an anti-counterfeit policy and procedure.	M	M	R	R	To ensure component authenticity refer to reference AA, Directive on NATO Supply Chain Security for COTS CIS Security Enforcing Products.
Section PDI2: Security Planning						
PDI2-1	The CIS Security requirements for the CIS are determined.	M	M	M	M	In conjunction with the CISOA, CISP and CISPIA and approved by the SAA.
PDI2-2	The CIS has a formal Concept of Operations (CONOPS) which illustrates use case scenarios.	M	M	R	R	
PDI2-3	The CIS is based on a SAA approved Security Architecture.	M	M	R	R	Using security engineering principles (e.g. ISO 27001 and NIST 80-27) in the specification design, development, and implementation of the CIS. Security Architecture: e.g. Reference Architecture; Target architecture
PDI2-4	Sufficient resources to protect the CIS are allocated.	M	M	M	M	Includes acquisition and Operations and Maintenance costs, both material and human costs.
PDI2-5	The protection of the supply chain is in accordance with reference AA or national equivalent.	M	M	M	M for NR	Reference AA: Directive on NATO Supply Chain Security for COTS CIS Security Enforcing Products

ID	Security Measure **Planning, Design and Implementation**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
PDI2-6	Security Accreditation for the CIS is in accordance with reference M.	M	M	M	M	Reference M: Management Directive on CIS Security
PDI2-7	The SecOPs are made available to all users of the CIS. Users formally acknowledge that they will comply with them.	M	M	M	M	E.g. signed (manually or digitally).
Section PDI3: Secure Acquisition Process						
PDI3-1	Security measures are detailed in organisational procurement contracts.	M	M	M	M	The CISPIA requires the CIS developer to provide adequate documentation and implementation information of the CIS Security enforcing components and their functional properties.
PDI3-2	The CISPIA and CISP manages the procurement of CIS Security capability throughout the CIS Lifecycle.	M	M	M	M	
PDI3-3	The CIS only uses evaluated and approved CIS Security enforcing products as identified in reference DD or national equivalent when available	M	M	M	M	Reference DD: Directive on Introducing Secure Systems and Solutions Using Commercial Off the Shelf (COTS) Products into NATO. Use products from the NIAPC where available. Security enforcing products in the categories of cryptographic equipment or emission security related equipment (TEMPEST) have to be approved by a NCSA as per reference P, Directive on Cryptographic Security, or reference T, Directive on Emission Security. Note: There are no TEMPEST restrictions on equipment processing NATO UNCLASSIFIED or NATO RESTRICTED information.

ANNEX 1
AC/322-D/0048-REV3 (INV)

ID	Security Measure **Planning, Design and Implementation**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
Section PDI4: External CIS providers						
PDI4-1	The CISPIA or CISP contractually requires external CIS service providers to comply with this directive.	M	M	M	M	Exceptions to this require SAA approval.
PDI4-2	Leased equipment, once used for storing or processing NATO Classified information, does not compromise the confidentiality of NATO information when returned.	M	M	M	M	For instance, hard drives wiped or hard drives removed and kept by NATO or a nation or leased equipment isn't returned but purchased instead. See PHM 8-1 for protection of storage media requirements.
Section PDI5: Implementation						
PDI5-1	Only appropriately security cleared or supervised personnel carry out the implementation of the CIS.	M	M	M	M	See PS2-1 and SMT2-4. If not appropriately cleared, Contractor personnel implementing the CIS are under the constant supervision of technically qualified NATO or national staff who are cleared for the highest classification of the information which the CIS handles or is expected to handle.

CIS SECURITY BREAKDOWN CATEGORY: SUSTAIN: EDUCATE TRAIN AND EXERCISE

D/0048 SECURITY MEASURE GROUP: SECURITY EDUCATION AND AWARENESS

CIS Security education and awareness shall be a prerequisite to system use in accordance with the requirements set forth in reference L, the Primary Directive on CIS Security. Users shall be educated on the importance of CIS protection and how to detect evidence of unauthorized activity, unusual events or incidents. Users shall be made familiar with relevant aspects of CIS SecOPs and understand their implications so that they may play their part in achieving CIS Security. Periodic security education and awareness shall be provided to users, system and security administrators. Security advisories and security alerts provided by the CISP (e.g. NCI Agency) or the Security Officer shall be taken into account when updating education on CIS threats.

This section corresponds to the following PILAR elements: Personnel: Training and Awareness.

ID	Security Measure **Security Education and Awareness**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
IMPORTANT: Read “Application of this Directive,” page 1-8, to understand the use of “M” and “R.”						
Section EA1: Policy						
EA1-1	The organisation implements a Security Education and Awareness policy and associated procedures.	M	M	R	M	

ANNEX 1
AC/322-D/0048-REV3 (INV)

ID	Security Measure **Security Education and Awareness**	NATO CIS		NATIONAL CIS handling NATO information		Remarks
		NC/NS/CTS	NU/NR	NC/NS/CTS	NU/NR	
Section EA2: Education						
EA2-1	CIS Security awareness education is provided annually to all users, and in their first month for new users.	M	M	M	M	Training may be done online or in a classroom.
EA2-2	CIS Security awareness education includes, as minimum, the following topics: • user incident reporting procedures; • email security including phishing; • web security; • mobile device security; • data protection; • malware; • social engineering; • and insider threat.	M	M	M	M	
EA2-3	Corrective action is taken against those who do not complete the required security training.	M	M	M	M	For instance, administrative action or termination of access to CIS until training is completed.
Section EA3: CIS Role based Education						
EA3-1	Comprehensive CIS Security role focused education is provided to privileged users and CIS Security personnel.	M	M	M	M	

GLOSSARY

1. **Access Control:** The process of granting or denying specific requests:
    a. For obtaining and using information and related information processing services; and
    b. To enter specific physical facilities (e.g., buildings, rooms).
2. **Anti-malware:** A term used to describe a set of security products aimed at detecting and removing malicious code. These products rely on signatures of known malicious code attacks to successfully detect them. More recently anti-malware products include heuristic capabilities allowing them to conduct behavioural analysis of potential malicious code, in attempts to identify new or unknown attacks for which signatures do not exist.
3. **Application Whitelisting:** A technology which permits or denies the execution of code on a computer system with the goal to protect the system and its environment from potentially harmful or malicious code.
4. **Asset:** Anything that has value to the organisation, its business operations and its continuity.
5. **Audit:** The routine, usually automated, review by the CISP of system logs to identify abnormalities and indicators of compromise. This is different than the Security Audit defined in reference M, Management Directive on CIS Security, due to its focus on continuous monitoring compared to the periodic Security Audits role in accreditation and security risk management.
6. **Audit Logs, Event Logs, or System Logs:** Logs that record user activities, exceptions, and CIS Security events, which are kept for an agreed period, to assist in future investigations and access control monitoring.
7. **Audit Trail:** The chronological record of auditable events relating to a specific item, which enables the reconstruction and examination of a sequence of events relating to that item.
8. **Authentication:** The means by which that identity is verified using an authenticator (e.g. password or token).
9. **Authenticator:** A password, PIN or device (e.g. token, smartcard) used to authenticate to a CIS system.
10. **Availability:** The property of being accessible and useable upon demand by an authorized entity.
11. **Baseline Configuration:** In configuration management, a "baseline" is an agreed description of the attributes of a product, at a point in time, which serves as a basis for defining change. An "alteration" is a movement from this baseline state to a next state. The identification of significant changes from the baseline state is the central purpose of baseline identification.
12. **Boundary Protection Component (BPC):** A component of a system that provides a Boundary Protection Service (BPS). E.g.: firewalls, data diodes, data guards, filtering routers, proxy servers, network intrusion preventers/detectors, content checking software at the interconnection.

13. **Boundary Protection Service (BPS):** A security service that mediates information flows or mitigates security risks introduced by a network interconnection. E.g. entity authentication, access control, packet checking, anti-malware.
14. **Captive Portal:** A webpage which is displayed to newly connected users before they are granted broader access to the Internet, as commonly used in Wi-Fi networks in hotels or cafés.
15. **Communications and Information System(s) (CIS):** Collective term for describing communications technology and information systems. Includes the physical environment (e.g. buildings, communications facilities and links, computer hardware); and information, data, software and service provision.
16. **CIS Operational Authority (CISOA):** The organisation using the CIS system to assist them in meeting their business and operational needs. In the CIS Security context, the CISOA is the residual risk owner. The CISOA responsibilities may be found in reference M, Management Directive on CIS Security.
17. **CIS Planning and Implementation Authority (CISPIA):** The organisation responsible for planning and fielding CIS systems, including the major upgrading of existing systems. This body may also be the CISP. The CISPIA responsibilities may be found in reference M, Management Directive on CIS Security.
18. **CIS Provider (CISP):** The organisation responsible for the operations and maintenance of CIS systems. This body may also be the CISPIA. The CISP responsibilities may be found in reference M, Management Directive on CIS Security.
19. **CIS Storage Media:** Analogue and digital storage media which may be portable (e.g. USB drives or CD-ROMs) or internal (e.g. hard drives).
20. **CIS Supporting Services:** Services essential for the running or protection of CIS services, such as electricity, air conditioning or fire suppression.
21. **CIS Users:** Employees or individuals who have equivalent status to employees within organisations (e.g. contractors, interns, members of national delegations to NATO, voluntary national contribution (VNC) manpower).
22. **Confidentiality:** The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
23. **Configuration Control:** The process of controlling modifications to a system's hardware, firmware, software and documentation to ensure that the system is protected against improper modification prior to, during and after system implementation.
24. **Configuration Management:** Management of security features and assurances through accurate asset inventories and control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of a CIS.
25. **Continuous Monitoring:** Near real time review of log data to detect situations detrimental to CIS Security, for instance attacks, unauthorized access, data leakage, or air conditioning failure.

26. **Credentials:** Evidence or testimonials that support a claim of identity or assertion of an attribute. An object that is verified when presented to the verifier in an authentication transaction. Credentials may be bound in some way to the individual to whom they were issued, or they may be bearer credentials. The former are necessary for identification, while the latter may be acceptable for some forms of authorization.
27. **Data at Rest:** Used to refer to all data in computer storage while excluding data that is traversing a network or temporarily residing in computer memory to be read or updated.
28. **Demilitarized Zone (DMZ):** sometimes referred to as a perimeter network, is a physical or logical sub-network that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet.
29. **Denial-of-service attack (DoS attack):** A cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. In a distributed denial-of-service attack (DDoS attack), the incoming traffic flooding the victim originates from many different sources. This effectively makes it impossible to stop the attack simply by blocking a single source.
30. **Device Sponsor:** Those responsible for obtaining PKI credentials required by system/network devices.
31. **General Data Protection Regulation (GDPR):** In regulation in European Union (EU) law on data protection and privacy for all individuals within the EU and European Economic Area (EEA).
32. **Health Insurance Portability and Accountability Act (HIPAA):** A USA law which among other things, stipulates how Personally Identifiable Information maintained by healthcare providers is protected from fraud and theft. HIPAA is one of the cornerstone privacy laws of the USA, despite its limited scope.
33. **Hypervisor:** Software and/or firmware running on the host that creates and controls all the virtual machines. It provides the virtual machine environment. The hypervisor layer between the hardware and virtual machine / guest OS has privileged access to layers above. It also has a great deal of control over hardware, and increasingly so, as hardware manufacturers implement hypervisor functions directly into chipsets and CPUs. Type 1 run directly on system hardware, sometimes referred to as “bare metal.” Type 2 run on a host OS that provides virtualization services such as I/O device support and memory management.
34. **Identification:** An act or process that presents an identifier to a system so the system can recognise a system entity (e.g., user, process, or device) and distinguish that entity from all others.
35. **Impact:** The effects on a business or business process should a threat be

realised, exploiting a vulnerability and causing a compromise to the integrity, availability or confidentiality of an information system.

36. **Integrity:** The property of safeguarding the accuracy and completeness of assets. This may include the ability to prove an action or event has taken place, such that it cannot be repudiated later.
37. **Interconnection:** The capability that enables the exchange of information between two CIS over an established connection. Note that a connection is defined in Allied Data Publication 02 as 'An association established between functional units for data transmission.'
38. **Least Privilege:** The system users are only given the privileges and authorizations they require to perform their tasks and duties.
39. **Logging:** The capture of security relevant CIS events.
40. **Malware (short for malicious software):** An umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other intentionally harmful programs. It can take the form of executable code, scripts, active content, and other software. Malware is defined by its malicious intent, acting against the requirements of the computer user and so does not include software that causes unintentional harm due to some deficiency.
41. **Mobile Code:** Code, such as a Java Applet, that is transmitted across a network (or storage media such as USB Flash Drives) and executed on a remote machine.
42. **Multi-factor or two-factor authentication:** A method of confirming a user's claimed identity in which a user is granted access only after successfully presenting 2 or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something they and only they know), possession (something they and only they have), and inherence (something they and only they are).
43. **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 to perform official tasks or services.
44. **Network Access Control (NAC):** NAC provides the ability to dictate the activities that identified users and devices are able to use on the CIS (typically using IEEE 802.1X). This included the ability to enforce network restrictions based on policies and procedures. NAC may include Network Access Protection (NAP) and Network Access Quarantine (NAQ) services.
45. **Password:** Protected/private alphanumeric string used to authenticate an identity or to authorize access to data.
46. **Peripheral Switch:** Either a Keyboard/Video/Mouse (KVM) or Data Switch. A KVM switch allows the use of one keyboard, monitor and mouse for more than one computer or server. A data switch routes one line to another – for instance to connect two computers to one printer. Shared peripheral switches may be either manual or automatic.
47. **Personally Identifiable Information (PII):** Data that could potentially identify a specific individual.

48. **Privileged Account:** An account with rights and access above that of a normal user (e.g. an administrator account.)
49. **Proxy Server:** A proxy server, also known as a "proxy" or "application-level gateway", is a computer that acts as a gateway between a local network (e.g., all the computers at one company or in one building) and an external network such as the Internet. Proxy servers provide security features such as blacklisting, whitelisting, malware checking, digital leakage prevention, or logging.
50. **Remote Access:** Access to the CIS from external networks not controlled by the organisation such as the Internet.
51. **Remote Maintenance:** Maintenance using remote access.
52. **Risk:** The potential that a given threat will exploit vulnerabilities of an asset and thereby cause harm to the organisation.
53. **Salt (cryptography):** Random data used as an additional input to cryptographic hashes in order to hinder rainbow table attacks on password hashes.
54. **Security Accreditation:** The process that determines that an adequate level of protection has been achieved and is being maintained. Central to this process is the identification of an acceptable level of residual risk which needs to be monitored throughout the CIS life-cycle.
55. **Security Accreditation Authority:** Official with the authority to issue a statement of security accreditation for CIS at an acceptable level of Risk to organisational operations (including mission, functions, image, or reputation), organisational assets, individuals, other organisations, and Nations, stating the conditions under which security re-approval or re-accreditation is required. The SAA responsibilities may be found in reference M, Management Directive on CIS Security.
56. **Security Attributes:** An abstraction representing the basic properties or characteristics of an entity with respect to safeguarding information; typically associated with internal data structures (e.g., records, buffers, files) within the information system which are used to enable the implementation of access control and flow control policies; reflect special dissemination, handling, or distribution instructions; or support other aspects of the information security policy.
57. **Security Audit:** The systematic review of a CIS to ascertain its susceptibility to compromise of the security objectives. A security audit can determine the susceptibility of a CIS to a specific attack, or determine the opportunity of a threat agent to exploit vulnerabilities. A security audit supports the security risk management or security accreditation process. Reference M, Management Directive on CIS Security, provides more details.
58. **Security Boundary:** A physical and/or logical border that defines the area of security responsibility of a CIS. This responsibility may also include the administration of the CIS.
59. **Security Domain:** A CIS or group of CIS as agreed by the SAA and CISOA. A Security Domain is defined, at least by, the security classification of the CIS or group of CIS. A Security Domain may also be defined by owner, responsible CISOA, responsible SAA, CIS owner, Community of Interest or Information

Domain.

60. **Security Modes of Operation:** Operating modes of a system, either;
    a. Dedicated – a mode of operation in which all individuals with access to the CIS are cleared to the highest classification level of information handled within the CIS, and with a common need-to-know for all of the information handled within the CIS.
    b. System high - a mode of operation in which ALL individuals with access to the system are cleared to the highest classification level of information stored, processed or transmitted within the system, but NOT ALL individuals with access to the system have a common need-to-know for the information stored, processed or transmitted within the system; approval to access information may be granted at an informal or individual level.
    c. Compartmented – a mode of operation in which ALL individuals with access to the system are cleared to the highest classification level of information stored, processed or transmitted within the system, but NOT ALL individuals with access to the system have a formal authorization to access ALL of the information stored, processed or transmitted within the system.
    d. Multi-level - a mode of operation in which NOT ALL individuals with access to the system are cleared to the highest classification level of information stored, processed or transmitted within the system, and NOT ALL individuals with access to the system have a common need-to-know for ALL of the information stored, processed or transmitted within the system.
61. **Security Objectives:** Confidentiality, integrity, availability, authentication, and non-repudiation, reference L, the Primary Directive on CIS Security.
62. **Security Operating Procedures (SecOPs):** Documented procedural countermeasures tailored to a specific user community designed to address particular risks. SecOPs should reflect local conditions, such as working practices, system configuration and environmental security constraints.
63. **Security Risk Assessment:** A structured and documented methodology of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact a CIS. Uses the results of threat and vulnerability assessments to identify risk to organisational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of a security risk assessment is a list of estimated, potential impacts and unmitigated vulnerabilities. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security measures planned or in place. The overall process of Risk Analysis and Risk Evaluation.
64. **Security Tools:** Software or hardware products that provide security management and services that enhance the security posture of a CIS.
65. **Self-Protecting CIS:** Each CIS treating other CIS as un-trusted and implementing protection measures to control the exchange of information with other CIS.
66. **Sender Policy Framework:** An email validation system designed to detect email

spoofing by allowing receiving mail exchangers to check incoming mail from a domain comes from a host authorized by that domain's administrators.

67. **Session Hijacking:** Session hijacking is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.
68. **Shared Account:** Account with one user name or identifier which are utilized by multiple users who share a single authenticator. An example is an authenticator for a ballistic missile defence monitoring system. It is unfeasible to log out and log in at shift change. Rather a procedure used to maintain accountability.
69. **Software Hardening:** A process which applies the appropriate security settings and group policies as well as disables nonessential software programs, services and utilities in order to minimize possible attacks.
70. **Split Tunnelling:** A VPN mode of operation where some of the data flows through the VPN and the rest of the data is able to flow to a different CIS, like the internet. The converse is forced tunnelling, where all the data flows through the VPN once it is established.
71. **Storage Area Network (SAN):** A high-speed network of storage devices that also connects those storage devices with servers. It provides block-level storage that can be accessed by the applications running on any networked servers. SAN storage devices can include tape libraries and disk-based devices e.g. RAID hardware.
72. **Storage Media:** diskettes, magnetic tapes, hard drives (including external/removable), SSD (Solid State Drive), USB flash drives, compact discs, and digital video disks (DVDs).
73. **Strength of (Cryptographic) Mechanism (SOM):** The potential of the mechanism to provide appropriate protection of information/systems against failures and threats posed by attackers having varying opportunity, expertise and resources (Reference P, Directive on Cryptographic Security, page 6)
74. **TEMPEST:** The investigation and study of compromising CIS equipment emanations is called TEMPEST (not an acronym). Compromising emanations are unintentional data-related or intelligence-bearing signals that, when intercepted and analysed, disclose classified information being transmitted, received, handled or otherwise processed by any information processing equipment. The term TEMPEST is also used to encompass these phenomena themselves and the measures for their suppression.
75. **Threat:** A potential cause of an incident that may result in harm to a system or organisation.
76. **Throttling (Login):** The introduction of pauses before a user can try to authenticate again. Designed to hinder guessing attempts by attackers. Account lock-out serves the same purpose, but throttling attempts to avoid the denial of service and subsequent service desk call associated with account lock-out.
77. **Tier 0 privileged users:** System Administrators who have direct control of organization identities in the environment. Tier 0 includes accounts, groups or indirect administrative control of the Active Directory forest (for Microsoft OS or

other OS equivalent), domains, or domain controllers, and all the assets in it. The security sensitivity of all Tier 0 assets is equivalent as they are all effectively in control of each other. Tier 0 accounts do not have Tier 1 or Tier 2 privileges. Tier 0 accounts are used very sparingly.

78. **Tier 1 privileged users:** System Administrators who control servers, applications and network devices. Tier 1 assets include limited privileges to Active Directory (or other OS equivalent), server operating systems, network devices such as routers or BPC, enterprise applications and application developers. Tier 1 administrator accounts have administrative control of a significant amount of business value that is hosted on these assets. A common example role is server administrators who maintain these operating systems with the ability to impact all organisational services. Tier 1 accounts do not have Tier 0 or Tier 2 privileges.
79. **Tier 2 privileged users:** System Administrators who control user workstations and devices. Tier 2 administrator accounts have administrative control of a significant amount of business value that is hosted on user workstations and devices. Examples include Help Desk and computer support administrators because they can impact the integrity of almost any user data. Tier 2 accounts do not have Tier 0 or Tier 1 privileges.
80. **Token:** Smart card, metal key, or other physical object used to authenticate identity.
81. **Traffic Flow Security (TFS):** The use of various measures or methods to hide the presence of messages across a communicational medium, or to otherwise cloak messaging to prevent Traffic flow analysis and the observation of traffic levels across the CIS.
82. **User:** Person or process authorised to access a CIS.
83. **User Remote Access:** user connection from organisationally uncontrolled network to organisational CIS.
84. **Virtual private network (VPN):** A service that extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network.
85. **Vulnerability:** A weakness of an asset or group of assets that can be exploited by one or more threats.
86. **Vulnerability Assessment:** Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.
87. **Web Services Security (WS-Security or WSS):** An extension to SOAP to apply security to Web services. It is a member of the Web service specifications and was published by OASIS.
88. **Wi-Fi:** Wireless Fidelity. Radio-based protocol that may be used in a wireless local area network.

ABBREVIATIONS AND ACRONYMS

BIND	Berkley Internet Name Domain
BIOS	Basic Input/Output System
BPC	Boundary Protection Component
BPS	Boundary Protection Service
C3B	Consultation, Command and Control Board
CA	Certification Authority (PKI)
CD	Compact Disk
CERT	Computer Emergency Response Team
CIS	Communication and Information System
CISOA	CIS Operational Authority
CISP	CIS Provider
CISPIA	CIS Planning and Implementation Authority
CM	Configuration Management - D/0048 Security Measure Group
CONOPS	Concept of Operations
COTS	Commercial Off-the-Shelf (products)
CP	Continuity Planning - D/0048 Security Measure Group
CPU	Central Processing Unit
CS	Control Systems - a D/0048 Security Measure Group
CTS	COSMIC TOP SECRET
DA	Data Protection - D/0048 Security Measure Group
DDoS	Distributed Denial of Service (attack)
DKIM	DomainKeys Identified Mail

DLL	Dynamic Link Libraries
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting and Conformance
DMZ	Demilitarized Zone in a network (perimeter network)
DNS	Domain Name System
DNSSEC	Domain Name Security Extensions
DoS	Denial of Service (attack)
DVD	Digital Video Disc or Digital Versatile Disc
EA	Security Education and Awareness - D/0048 Security Measure Group
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload
FC	Fibre Channel
GDPR	General Data Protection Regulation
HIDS	Host-based Intrusion Detection System
HIPAA	Health Insurance Portability and Accountability Act
IAM	Identity and Access Management. Also a D/0048 Security Measure Group
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
INFOSEC	Information Security
I/O	Input/Output
IP	Internet Protocol

IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IR	Incidence Response - D/0048 Security Measure Group
ISO	International Organization for Standardization
KVM	Keyboard/Video/Mouse
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LMA	Logging, Continuous Monitoring and Audit - D/0048 Security Measure Group
LUN	Logical Unit Number
NCI Agency	NATO Communications and Information Agency
M	Mandatory (Security Measure)
MAC	Media Access Control
NAC	Network Access Control
NAP	Network Access Protection
NAQ	Network Access Quarantine
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
NC	NATO CONFIDENTIAL
NCSA	National Communications Security Authority
NIAPC	NATO IA Product Catalogue
NPMA	NATO PKI Management Authority
NR	NATO RESTRICTED

NS	NATO SECRET
NSAB	NATO CIS Security Accreditation Board
NTP	Network Time Protocol
NWS	Network Security - D/0048 Security Measure Group
NU	NATO UNCLASSIFIED
OASIS	Organization for the Advancement of Structured Information Standards
OS	Operating System
OTP	One Time Password
PDI	Planning, Design and Implementation - D/0048 Security Measure Group
PE	Physical and Environmental Security - D/0048 Security Measure Group
PHM	Protection of Hardware – D/0048 Security Measure Group
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
POS	Protection of Software - D/0048 Security Measure Group
PS	Personnel Security - D/0048 Security Measure Group
PSCS	Physical Security Control System
PSW	Protection of Software - D/0048 Security Measure Group
PTP	Precision Time Protocol
QoS	Quality of Service

R	Recommended (Security Measure)
RAID	Redundant Array of Independent Disks
SAA	Security Accreditation Authority
SAN	Storage Area Network
SCADA	Supervisory Control and Data Acquisition
SCIP	Secure Communications Interoperability Protocol
SECAN	Military Committee CIS Security and Evaluation Agency
SecOPs	Security Operating Procedures
SM	Security Measure
SMS	Short Message Service
SMT	Secure Maintenance - D/0048 Security Measure Group
SOAP	Simple Object Access Protocol
SOM	(Cryptographic) Strength of Mechanism
SPF	Sender Policy Framework
SQL	Structured Query Language
SRA	Security Risk Assessment
SSD	Solid State Drive(s)
TEMPEST	Not an acronym, rather a code word for emission security protection measures.
TFS	Traffic Flow Security
TLS	Transport Layer Security
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus

VLAN	Virtual LAN
VM	Virtual Machine(s)
VoIP	Voice over IP
VPN	Virtual Private Network
WAF	Web Application Firewalls
Wi-Fi	Wireless networking (pun on hi-fi – high fidelity)
WIPS	Wireless Intrusion Protection System
WPA2	Wi-Fi Protected Access Version 2
WSS	Web Services Security
WWN	Worldwide Name Number
XSS	Cross Site Scripting