NORTH ATLANTIC TREATY ORGANIZATION
ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD
HEADQUARTERS SUPREME ALLIED COMMANDER TRANSFORMATION
7857 BLANDY ROAD, SUITE 100
NORFOLK, VIRGINIA, 23551-2490

2000/ TSC-MVX-0010/TT-0452/Ser:NU

TO: See Distribution

SUBJECT: **ENHANCING THE PROTECTION OF NATO RELATED NETWORKS WITHIN NATO COES**

DATE: 31 October 2018

REFERENCES: A. MCM-0253-2017, NATO Military Authorities' Advice on Enhancing the Protection of NATO Related Networks, 05 Dec 17.
B. PO(2018)0037, Approval of the Advice on Enhancing the Protection of NATO Related Networks, 29 Jan 18.
C. IMSM-0136-2018, Strategic Commands' Responses to the MC Tasking on Enhancing the Protection of NATO Related Networks, 19 Mar 18.
D MCM-0114-2018 MILITARY COMMITTEE FOLLOW-ON ADVICE ON ENHANCING THE PROTECTION OF NATO RELATED NETWORKS
E. MCM-236-03, MC Concept for Centres of Excellence, 04 Dec 03.
F. IMSM-0416-04, NATO Centres of Excellence Accreditation Criteria, 11 Jun 04.
G. AC/322-D(2017)0047, Minimum Requirements of Cyber Defence for the Protection of NATO Related Networks.

1. On the 05 December 2017 the Military Committee (MC) approved the NATO Military Authorities' advice on enhancing the protection of NATO Related Networks (Reference A). With this initial advice, as noted and supported by the Council at Reference B, the MC assigned a number of tasks to the Strategic Commands (SCs) to take the initial steps towards enhancing the protection of NATO Related Networks. As a result, the SCs provided their responses (Reference C), leading to further taskings under Reference D.

2. In accordance with Reference B, NATO Related Networks are defined as those that fulfil all of the following criteria:

a. Handle NATO UNCLASSIFIED information and/or Information Releasable to the Public.

b. Fall under national/multinational responsibility for their cyber defence.

c. Are not covered by NATO's centralized protection.

d. Operate under a Memorandum of Understanding (MoU) or Memorandum of Agreement (MoA) with NATO and/or are co-located with NATO civil or military bodies.

e. If compromised, would present, at the very least, a reputational risk to NATO.

3. Reference D notes that, whereas cyber defence for NATO Related Networks is an important and urgent requirement, changes to References E and F, and to the Functional MoU governing each of the NATO Centres of Excellence may not be immediately feasible (note that the revision of References E and F is ongoing). Accordingly I am writing to you to request that you implement the measures prescribed in Reference D at your earliest opportunity. To assist with these efforts, Annex A summarizes the proposed changes to Reference E and F, and to the functional MoUs. Annex B contains details of the required technical measures, extracted from Reference G. HQ SACT will ensure that the language proposed in Annex A (and approved at Reference B) is included in new Functional MoUs and included in current Functional MoUs when Functional MoUs are subject to revision.

4. Specifically, I request that each COE should:

a. Inform HQ SACT of the National Security Oversight Authority identified by your nations to conduct security oversight of your COE;

b. In coordination with the identified National Security Oversight Authority, conduct an annual assessment to validate compliance with Reference G (summarised in Annex B) and provide a signed written statement of compliance with the referenced minimum requirements to HQ SACT – Transformation Network Branch annually.

5. Should there be any questions, our point of contact is Commander Cesar CORREIA, +1(757)747 3348, cesar.correia@act.nato.int.

FOR THE SUPREME ALLIED COMMANDER TRANSFORMATION:

Paul Bennett

Paul M Bennett CB OBE
Vice Admiral, GBR N
Chief of Staff

ANNEXES:

A. Changes to the MC Concept for Centres of Excellence, NATO Centres of Excellence Accreditation Criteria and NATO Centres of Excellence Functional MOUs
B. Minimum Requirements of Cyber Defence for the Protection of NATO Related Networks

DISTRIBUTION:

External –

Action:

List VIII

Information:

Members of the Security Committee (AC/35), via NOS

Internal –

Information:

DCOS CAPDEV
DCOS RM
ACOS REQS
LEGAL

ANNEX A TO
2000/ TSC-MVX-0010/TT-0452/Ser:NU
DATED 3 OCT 18

Changes to the MC Concept for Centres of Excellence, NATO Centres of Excellence Accreditation Criteria, and NATO Centres of Excellence Functional MOUs

1. Reference D directs ACT to include the following changes in the next revision of the respective documents.

MC Concept for Centres of Excellence,

2. "A CoE is to conform with appropriate NATO procedures, doctrines and standards, including safety and security."

NATO Centres of Excellence Accreditation Criteria

3. "Safety and Security. Safety and security of visiting and assigned personnel must be provided in accordance with appropriate NATO standards and regulations. The CoE must also ensure that appropriate safety procedures and properly functioning equipment are in place, well maintained and operated by trained personnel. The CoE must employ adequate security measures to safeguard designated information, materiel, personnel, activities and installations.

4. Adequacy of the security measures will be assessed based on (a) a summary of the findings of the periodic review by the designated bodies of all security within the CoE; and (b) written statements of compliance with appropriate technical standards, signed by the designated bodies."

NATO Centres of Excellence Functional MOUs

5. "The Head of the [MoU/MoA Entity] is ultimately responsible for security within his/her organisation.

6. Security oversight of [MoU/MoA Entity] will be provided by [Host Nation] through [National Security Oversight Authority].

6. In order to protect NATO information, to safeguard NATO's reputation, and to ensure adequate protection of NATO related networks, [Host Nation] will ensure that the [MoU/MoA Entity] understand their obligation to comply with the applicable requirements established in all relevant NATO policies, paying special attention to the requirements established in the current version of AC/322-D(2017)0047, Minimum Requirements of Cyber Defence for the Protection of NATO Related Networks, Annex 1, Appendix 1, first approved 15 Nov 17.

7. To ensure compliance with these standards, [National Security Oversight Authority] will conduct an initial and thereafter periodic review of all security within [MoU/MoA Entity] as

prescribed by national regulations. Moreover, the [Host Nation] will ensure that the [National Security Oversight Authority] and [MoU/MoA Entity] will conduct an annual assessment to validate compliance and provide a signed written statement of compliance with the referenced minimum requirements to [Placeholder- insert appropriate NATO entity] annually."

ANNEX B TO
2000/ TSC-MVX-0010/TT-0452/Ser:NU
DATED 31 OCT 18

Minimum Requirements of Cyber Defence for the Protection of NATO Related Networks

The tables below are extracted from the current version of AC/322-D(2017)0047, Minimum Requirements of Cyber Defence for the Protection of NATO Related Networks, Annex 1, Appendix 1, first approved 15 Nov 17.

Cyber Defence Requirements	M / R[1]	Remarks
1. PREVENT		
1.1. Communication & Information Systems (CIS) Protection		
1.1.1. Firewalls to limit the network traffic to a defined and managed set of network ports	M	
1.1.2. Email gateways which are capable of scanning incoming emails for malicious code, with regularly updated signatures for detecting such code	M	
1.1.3. Software solutions deployed at the endpoint systems to control the installation, spread and execution of malicious code, for which the signatures for detection are updated at least once per day (e.g. antivirus products)	M	
1.1.4. Measures (dedicated software or through configuration) to limit and control the introduction of external devices to the endpoints and ensure that only authorised devices can be connected	M	

[1] (M)andatory or (R)ecommended

Cyber Defence Requirements	M / R[1]	Remarks
1.1.5. Firewalls which can apply filtering at the application layer for a more fine-grained control of incoming and outgoing network traffic	R	
1.1.6. Measures to limit and control the introduction of devices to the network infrastructure (e.g. by implementing certificate based network access control)	R	
1.1.7. Measures to implement web content filtering (e.g. reverse web proxies)	R	
1.1.8. Measures to mitigate Denial of Service attacks	R	
1.1.9. Host Intrusion Prevention software deployed on every endpoint to provide behaviour based detection of malicious activity to better mitigate against known, as well as emerging (including zero-day) attacks	R	While this is quite an effective security control, it should be considered as part of a defence-in-depth strategy, complementing other intrusion detection and prevention controls as reflected in 2.1.5 below
1.2. Data Protection		
1.2.1. Measures to protect against unauthorised disclosure of Personally Identifiable Information (PII) (e.g. mandatory compliance with the General Data Protection Regulation (GDPR) where applicable)[2]	M	

[2] Note that in the view of the Strategic Commands, the GDPR is not enforceable against NATO. However, similar national data protection regulations may be applicable. With or without an applicable regulation, PII should be protected.

Cyber Defence Requirements	M / R[1]	Remarks
1.2.2. Measures to periodically scan the network, including the endpoints, in order to detect existence of classified information to identify and mitigate spillages and cross-domain violations	M	While the frequency is not specified, it is recommended to have such checks at least once a month
1.2.3. Data loss prevention mechanisms to be deployed on endpoints and/or network boundaries	R	Such mechanisms can be very effective in detecting the existence of classified information and preventing its leakage
1.3. Identity & Access Management		
1.3.1. Identification and authentication mechanisms to ensure only authorised users have access to the CIS and the information contained within	M	
1.3.2. Measures to manage the lifecycle of user, system and application accounts, their creation, use and deletion, applying the least required privilege principle	M	
1.3.3. Advanced identification and authentication mechanisms that provide a higher level of assurance of ensuring only authorised users have access (i.e. implementing multi-factor authentication)	R	
1.4. Asset & Configuration Management		
1.4.1. Measures to maintain secure configurations for all hardware and software, by applying security patches in a timely manner	M	
1.4.2. Measures to restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services	M	There are varying levels of detail in which one can implement this important control. The level of restrictions for non-essential functionalities should

Cyber Defence Requirements	**M / R[1]**	**Remarks**
		be determined as a result of risk assessment. The 'hardening' requirements for national unclassified networks could be used as guidance in this regard
1.4.3. Established change management processes to track, review, approve/disapprove, and audit changes to information systems	R	
2. DEFEND		
2.1. Detect		
2.1.1. Tools to monitor and log activity within the network	M	The level of detail for logging is intentionally not specified. Whatever the level chosen, this control shall not breach any applicable data protection regulations
2.1.2. Tools to monitor and log activity on the endpoints, to include servers	M	
2.1.3. Standard procedures and processes for the users of the CIS to report any computer or network anomalies they may notice	M	
2.1.4. A capability (person or a team) that will analyse any reported (by automated tools or by end-users) suspicious activity and decide whether it should be handled as an incident	M	
2.1.5. Intrusion Detection devices that are regularly updated with signatures to detect malicious activity in the networks	R	
2.1.6. Specialized network appliances that allow 'full packet capture' functionality, triggered by suspicious network activity, to enable detailed post-incident investigation within an acceptable time delay	R	

Cyber Defence Requirements	**M / R[1]**	**Remarks**
2.1.7. Specialized software deployed on endpoints, to be triggered on demand, allowing for capturing forensic images of storage and memory devices	R	
2.2. Respond		
2.2.1. Documented incident handling and response procedures that include a definition of roles and phases for handling incidents	M	
2.2.2. A capability (designated person or team) to execute the incident handling and response procedures when necessary	M	
2.2.3. A set of contingency plans to be applied in case of incidents	M	
2.2.4. Designated personnel trained in digital forensics procedures, to undertake activities related with the identification, collection and preservation of digital information on security incidents	R	
2.3. Recover		
2.3.1. Measures and the ability to restore CIS to fully operational status, restoring system and information integrity, and service availability	M	
2.3.2. Pre-agreed and documented prioritization of which systems are most critical for urgent recovery	R	
2.3.3. Pre-defined lists of critical systems that should not be impacted, as well as critical data that should not be lost when executing recovery procedures	R	

Cyber Defence Requirements	M / R[1]	Remarks
3. ASSESS[3]		
3.1. Manage Risk		
3.1.1. Procedures to continuously assess the risk to organisational operations (including mission, functions, image, or reputation), resulting from potential exploitation of CIS vulnerabilities	M	These two mandatory requirements refer to the adoption of a risk management approach to CIS Security and cyber defence as is mandated by NATO Security Policy
3.1.2. Established procedures to assess and accept / mitigate / transfer the identified risks	M	
3.2. Assess Cyber Defence of Communication and Information Systems		
3.2.1. A capability (designated person or team) to conduct cyber defence assessments on a periodical basis to discover the vulnerabilities and exposures of CIS	M	It is recommended to conduct detailed assessments at least once a year. In case the designated person or team has the specialised tools to conduct automated vulnerability assessments, this frequency can be increased in order to quickly identify known vulnerabilities and mitigate them
3.2.2. A capability (person or a team) to support the change management process by conducting security assessments (including scanning for vulnerabilities, detecting bad practices of development, also conducting penetration testing) on any software or hardware that is being evaluated for approval before deployment on the network	R	

[3] In line with the recommended self-assessment approach, any assessments or audits referred to within this section will be conducted by the Host Nation of the NATO related network in question.

Cyber Defence Requirements	M / R[1]	Remarks
3.3. Audit		
3.3.1. Periodical security audits and inspections to verify that the cyber defence of the NATO related network is in compliance with the minimum requirements laid out within this document.	M	In line with the recommended self-assessment approach, this should be conducted by the the Host Nation of the NATO related network in question. The periodicity of this audit and verification should be aligned with the specific agreement to be captured within the MoU / MoA

Cyber Defence Requirements	M / R[1]	Remarks
4. SUSTAIN		
4.1. Educate, Train, and Exercise		
4.1.1. Education and awareness programmes that leverage the use of digital as well as printed media to ensure end-users are made aware of the general threats and vulnerabilities applicable to the CIS they use, in order that they acknowledge their responsibility to maintain the protective security measures in place and adopt 'cyber hygiene' in their way of working	M	
4.1.2. Recurring training for personnel responsible for executing cyber defence activities	M	While one can provide dedicated cyber defence training opportunities to personnel, it is also possible to incorporate cyber defence training into the overall training and education programmes (e.g. network and system administrators training)
4.1.3. Participate in NATO exercises focusing on cyber defence, giving their personnel the opportunity to witness and act within the context of simulated cyber threat/attack/crisis scenarios	R	

Cyber Defence Requirements	M / R[1]	Remarks
5. INFORM		
5.1. Collect		
5.1.1. Means for the personnel responsible for detecting incidents, to access all security related logs spread throughout the network	M	
5.1.2. Specialized software and / or appliances (e.g. a Security Incident and Event Management tool and its sub-components for log aggregation) to automatically collect all relevant logs in a central repository to facilitate analysis	R	Since the cyber defence of NATO related networks fall under national responsibility, this centralised collection of security logs should be conducted by the relevant national entities (e.g. national Computer Emergency Response Teams)
5.2. Analyse		
5.2.1. A capability (person or a team) with the required training to conduct post-incident analysis activities, leveraging the information collected from the networks, to conduct root cause analysis and identify user mistakes, unpatched vulnerabilities or potential gaps in preventive mechanisms that may have led to the incident	M	
5.3. Evaluate		
5.3.1. A capability (person or a team) and the required tools to evaluate security information collected through long periods, to enable correlation and trends analysis, to be complemented with threat information in order to achieve cyberspace situational awareness.	R	

Cyber Defence Requirements	M / R[1]	Remarks
5.4. Report & Share		
5.4.1. Standard procedures and processes to share information about cyberattacks and incidents affecting NATO Related Networks, and the information contained therein, with NATO	M	The Host Nation responsible for the NATO related network should share, as soon as possible, information about cyberattacks and incidents affecting the network, and the information contained therein, with NATO (e.g. NATO cyber defence POC identified within the MoU / MoA)