EUROPEAN
COMMISSION

Brussels, 26.10.2018
C(2018) 7284 final

IT Security Standard

IT Vulnerability and Remediation Management

Contents

1. INTRODUCTION

1.1. Legal Base

This IT security standard is based on Commission Decision (EU, Euratom) 2017/46 on the security of communication and information systems in the European Commission and Commission Decision laying down implementing rules for Articles 3, 5, 7-15 of Decision 2017/46, C (2017) 8841, in particular its Article 12.

It repeals the IT Security Standard on Vulnerability Management related to Commission Decision C(2006) 3602.

1.2. Subject matter and scope

1. The subject matter and scope of this IT Security Standard are provided in Article 1 of Decision (EU, Euratom) 2017/46.

2. The provisions in this IT Security Standard apply to all IT systems in the Commission. The relevant responsibilities and security measures for IT systems handling EU classified information shall be in line with Decision (EU, Euratom) 2015/444.

3. The principles of IT Vulnerability and Remediation Management shall also apply to outsourced IT systems and shall be documented in bilateral agreements or contracts with the Commission.

1.3. Definitions

For the purposes of this IT Security Standard, in addition to the definitions in Article 2 of Commission Decision (EU, Euratom) 2017/46 and in Article 2 of Commission Decision (EU, Euratom) 2017/8841 the following definitions also apply:

1) 'IT Asset Management' means the systematic process to guide the planning, acquisition, operation and maintenance, renewal and disposal of IT assets.
2) 'IT Vulnerability' means a weakness or a missing control on an IT system that could be exploited by an IT security threat.
3) 'Network and host vulnerability scanning' means vulnerability scanning for network, and all components of an IT system, except the application.
4) 'Patch' or 'Software Patch' means a piece of software/firmware designed to update a computer program or its software configuration, to fix or improve it.
5) 'Patch and Vulnerability Group' means the entity or team responsible for performing and orchestrating IT vulnerability and remediation management processes for the IT systems and technologies in scope. DIGIT is the principle patch and vulnerability group within the Commission.
6) 'Remediation measure' means a workaround or final solution to eliminate fully or partially an IT vulnerability by the installation of a software patch, hardware upgrade, process or procedural changes, adjustment of a configuration setting, and/or removal of affected software.

2. PROCESS, ORGANISATION AND RESPONSIBILITIES

2.1. IT Vulnerability and Remediation Management

1. IT vulnerability and Remediation management is a security practice designed to identify and remediate vulnerabilities in a timely way. The objectives are to prevent proactively the exploitation of IT vulnerabilities that exist within IT systems and to validate the proper execution of the regular patching process.

2. A dedicated Commission remediation database shall contain remediation measures that need to be applied for the IT technologies that are widely used within the Commission.

3. The IT vulnerability and Remediation management process is divided into two phases, namely identification and response, where at each step, appropriate communication is released to relevant stakeholders:

   a) Identification phase: monitor security sources for vulnerability announcements, remediation measures, and emerging IT security threats; perform IT vulnerability assessments; and analyse possible remediation.

b) Response phase: prioritizing, testing, implementing and monitoring of IT vulnerability remediation measures; exception handling.

4. Identification phase shall use at least one type of the following resources to ensure accurate and timely information about new vulnerabilities or emerging IT security threats:

   a) Vendor web sites, information feeds and mailing lists

   b) Third-party web sites (e.g. CERT-EU), mailing lists, newsgroups and social media

   c) IT vulnerability scanners and databases

   d) Enterprise patch management tools

   e) Other notification tools and methods

5. In accordance with the priority levels[1] as described in appendix 2, assessments to identify vulnerabilities in IT systems and IT services shall include regular performing and reporting on:

   a) Authenticated IT vulnerability scanning – Baselining the vulnerability posture, identifying un-patched systems when logged in as a user or privileged user on the IT system.

   b) IT vulnerability scanning – Baselining the vulnerability posture, identifying unpatched systems.

   c) Configuration Reviews – Automated and/or manual validation of adequate usage of security baseline configurations for application, server O/S, network and end user systems.

   d) Code review – Automated and/or manual validation of software code based on pre-defined IT security criteria and rules.

   e) Security Tests (e.g. ethical penetration testing) – verification, through provision of objective evidence, of the effectiveness of the security controls implemented or to validate an identified weakness.

6. Appropriate management of IT vulnerabilities reduces exposure by assuring that:

   a) Prioritisation of vulnerability remediation shall be the result of considering each IT security threat and its potential impact on the Commission.

   b) Remediation testing shall, where feasible, evaluate all remediation measures in a test environment before being pushed into production.

   c) Remediation implementation shall, where feasible, apply all remediation measures.

   d) Remediation monitoring shall ensure the effectiveness over time of the remediation implementation by repeated vulnerability scanning.

   e) Exception handling shall ensure that all remediation exemption requests are reviewed on a regular basis, assessed, and approved by the relevant stakeholders.

   Lessons shall be taken from the IT security vulnerability process once the remediation measure is successfully applied. This shall enforces continuous improvement of IT security, in particular IT vulnerability and remediation management activities.

2.2. IT Vulnerability and Remediation Management Roles and Responsibilities

1. Head of Commission Departments are accountable for the IT vulnerability and remediation management in their IT systems.

[1] For more information on priority levels of IT systems and their IT assets we refer to the IT Asset Management Security Standard

2. Each Head of Commission Department shall ensure, with the support of DG DIGIT, that the appropriate processes and procedures are in place to ensure efficient and effective IT vulnerability and remediation management related to their IT systems.

3. The System Owner or System Managers with delegated responsibilities shall:

   a. assign a patch and vulnerability group;

   b. ensure their IT systems are not exposed to known vulnerabilities by having:

      i. A Patch and Vulnerability Group regularly perform assessments to identify vulnerabilities in their IT systems and IT services and that reporting, to the system owner, on the Patch and Vulnerability Group activities is performed, in particular running automated IT vulnerability scanning tools against all their systems on the network;

      ii. Testing of IT vulnerability remediation measures conducted on test IT systems that use configurations that are as close as possible to the production ones;

      iii. IT vulnerability remediation measures deployed in a timely manner, and whenever possible, using enterprise management tools;

   c. collaborate with DG DIGIT to ensure IT vulnerability and remediation management activities are performed in an efficient way;

   d. collaborate with the DG DIGIT patch and vulnerability group in a timely manner to facilitate remediation implementation for IT systems and IT services provided by DG DIGIT;

   e. consider the implementation of other mitigating measures, when patches are not readily available, or deployment has unacceptable adverse impact on business, in particular:

      i. Network or proxy filtering.

      ii. Increased monitoring.

      iii. Awareness training/communications.

      iv. Temporarily disabling impacted services/features.

      v. Organisational, process or procedure adaptation

   f. test remediation measures in non-production systems, except where unfeasible ,;

   g. approve in a formal manner any decisions to delay remediation measures based on business requirements or identified risk to business stakeholders; and accept the related residual risks;

   h. request formal remediation exceptions to DG DIGIT, for IT systems or IT services provided by DIGIT, based on business needs or identified IT risks;

   i. register remediation exceptions in the Commission Remediation Database for the IT technologies that are widely used within the Commission;

4. System Managers, System Suppliers and IT Service Providers, with delegated responsibilities from the System Owner, shall ensure that patches are applied in accordance with the relevant change control procedures and shall perform, where feasible, authenticity, integrity and anti-virus testing for the downloaded patches.
5. The LISO shall advise the System Owner on IT vulnerability and remediation management, and support the Head of Department.
6. DG DIGIT, as the principle Patch and Vulnerability Group within the Commission, shall for IT technologies that are widely used within the Commission:

   a) with the support of System Suppliers, document a list of IT technologies that are widely used within the Commission and that are supported by Commission database of remediation measures and make the list available to the System Owners;

b) with the support of System Suppliers and System Managers, create and maintain the Commission database of remediation measures and their status;

c) with the support of System Suppliers, monitor security sources for vulnerability announcements, remediation measures, and emerging IT security threats and list suggested remediation measures of in the Commission database remediation measures;

d) with the support of System Suppliers and System Managers, advise on order of prioritization in which the Commission shall address remediating vulnerabilities;

e) oversee the vulnerability remediation process;

f) inform System Owners of vulnerabilities and remediation measures;

g) verify vulnerability remediation through network and host vulnerability scanning;

h) provide assistance and advice to System Owners and LISO's in their IT vulnerability and remediation management activities;

i) test remediation to avoid the need for redundant testing by each System Owner;

j) report on request, to the ISSB on the IT vulnerability and remediation management exceptions received from business stakeholders for the IT technologies supported by the Commission Remediation Database.

7. DG DIGIT shall escalate persistent non-compliance with this standard to the ISSB.

8. DG DIGIT shall perform vulnerability scanning, testing and timely remediation for all IT systems and IT services provided by DIGIT and Systems Owners shall be informed of vulnerability scanning campaigns and of their results. System Owners willing to opt out from those IT vulnerability assessments shall ask for formal approval to DIGIT.

3. MISCELLANEOUS AND FINAL PROVISIONS

3.1. Transparency

This IT Security Standard shall be brought to the attention of Commission staff and to all individuals to whom it applies.

3.2. Technical Standards

1. The provisions of this IT Security Standard shall, where necessary, be further detailed in technical standards and/or guidelines to be adopted in line with Commission Decisions 2017/46 and its implementing rules C(2017) 8841. These technical standards and guidelines shall be based on industry best practices and are selected to suit the Commission's IT environment.

2. The Security Standard on Vulnerability Management and related guidelines adopted under Decision C (2006) 3602 of 16 August 2006 are repealed.

3.3. Entry into force

This standard shall enter into force on the day following the date of adoption of this standard.

Appendix 1: Roles & Responsibilities (RASCI)

Role: / Activity	Head of Commission Department	System Owner	System Manager	DIGIT	System Supplier/ IT Service Provider	LISO	ISSB
Monitoring Vulnerabilities	**A**	**R**	**R(D)[2]/S**	**R(D)[3]/S[3]**	**S**		
Remediation measures and Threats analysis	**A**	**R**	**R(D)[2]/S**	**R(D)[3]/S[3]**		**S/C**	
Vulnerability assessments	**A**	**R**	**R(D)[2]/S**	**R(D)[3]/S[3]**	**S/C**		
Prioritizing Vulnerability Remediation	**A**	**R**	**R(D)[2]/S**	**R(D)[3]/S[3]**	**S**		
Remediation testing	**A**	**R**	**R(D)[2]/S**	**R(D)[3]/S[3]**			
Remediation deployment	**A**	**R**	**R(D)[2]/S**	**R(D)[3]/S[3]**	**R(D)1/S**		
Remediation Monitoring	**A**	**R**	**R(D)[2]/S**	**R(D)[3]/S[3]**			**I**
Exception Handling	**A**	**R**	**R(D)[2]/S**	**S[3]**		**S**	**I**
Lesson Learned	**A**	**R**	**R(D)[2]/S**	**S[3]**		**S**	**I**

'RASCI' is an abbreviation for a responsibility assignment based on the following attribution indicators:

(a) 'responsible' (R) means having the obligation to act and take decisions to achieve required outcomes;
(b) 'accountable' (A) means being answerable for actions, decisions and performance;

(c) 'supports' (S) means having the obligation to work with the person responsible to complete the task;

(d) 'consulted' (C) means being sought for advice or opinion;

(e) 'informed' (I) means being kept up to date with relevant information.

[2] With Delegated Responsibility from the System Owner
[3] With Delegated Responsibility from the System Owner for the IT technologies widely used within the Commission or in the role of principle Patch and Vulnerability Group within the Commission

Appendix 2: Assessments to identify vulnerabilities per priority labels[4] table

Assessment / Priority Label	IT Vulnerability Scanning	Authenticated IT Vulnerability Assessment	Configuration and Code review	Security Tests (Blackbox)
Very High	Mandatory	Mandatory	Mandatory	Mandatory
High	Mandatory	Mandatory	Mandatory	Recommended
Major	Mandatory	Mandatory	Recommended	Recommended
Medium	Mandatory	Recommended		
Low	Mandatory			

[4] For more information on priority levels of IT systems and their IT assets we refer to the IT Asset Management Security Standard