EUROPEAN
COMMISSION

Brussels, 16.11.2021
C(2021) 8428 final

Standard under Commission (EU, Euratom) 2017/46

External network connections

Table of Contents

1. Introduction 2

2. Scope 2

3. Definitions 3

4. Risks of external network connections 4

5. Connection types 4

6. Interconnection security agreement 5

7. Security measures 6

7.1. Rules for all external connections to Commission CISs 6

7.1.1. Governance 6

7.1.2. Network access services 6

7.1.3. Security perimeter services 8

7.1.4. Authentication and session management 8

7.1.5. End devices 8

7.1.6. Access to CISs 8

7.2. Rules for baseline connections 9

7.3. Rules for custom connections 9

8. External and remote users 10

9. RASCI matrix 10

1. INTRODUCTION

Article 6(5) of Commission Decision (EU, Euratom) 2017/46[1] assigns the following responsibility to DG HR:

> *"establish a framework for the authorisation of access and the associated appropriate security rules to Commission CISs from external networks and develop the related IT security standards and guidelines in close cooperation with the Directorate-General for Informatics;"*

This is further detailed in Article 7 of the implementing rules for that article, Commission Decision (EU, Euratom) 2018/559[2].

External network connections are defined as either **baseline connections** or **custom connections**. Baseline connections are those that are established in line with the baseline rules given in this document or in additional baselines that may be published by HR.DS. Custom connections require an interconnection security agreement (ISA), which is a formal agreement between all relevant parties on the necessary security rules. This document describes the roles and responsibilities involved in this process and lays out high-level rules for connections between Commission communication and information systems (CISs) on the internal network and external networks. Additional security baselines laying down requirements for specific scenarios involving an external network connection and a use case may be issued under this standard by HR.DS.

External network connections are established to allow users or externally located CISs to access one or more Commission CISs on the internal network[3]. Consequently, this document also includes high-level rules for users and for the system owners of the Commission CISs that are accessed.

Due to the varied nature of custom connections, different rules will apply to different types of connections. The applicable rules will be documented in the ISA for each of these connections.

2. SCOPE

The scope covers all connections with Commission CISs on the internal network that traverse one or more network segments that are not controlled by the Commission. This includes connections with:

- Commission CISs hosted outside Commission premises (including cloud environments);
- third party CISs;
- networks on external premises used by Commission staff or contractors
- users working via remote access; and
- external users accessing Commission CISs.

This definition excludes:

---

[1] Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission, OJ L 6, 11.1.2017, p.40.

[2] Commission Decision (EU, Euratom) 2018/559 of 6 April 2018 laying down implementing rules for Article 6 of Commission Decision (EU, Euratom) 2017/46 on the security of communication and information systems in the European Commission, OJ L 93, 11.4.2018, p.4.

[3] The internal network is defined as the data network infrastructure that interconnects the entire ICT infrastructure installed in the Commission´s premises, including the possible interfaces that enable the inter-building connection with external networks.

- internal network connections such as wide area network (WAN) links between Commission buildings, which are considered to be part of the internal network;
- connections between networks controlled by the network service provider, traversing exclusively segments under the control of the network service provider; and
- connections between Commission CISs hosted outside Commission premises and any external networks.

3. DEFINITIONS

The following terms are used in this document, including the roles that are involved in authorising and implementing external network connections. Where a role is already defined elsewhere, the reference is given in a footnote. Other roles are specific to this document.

System owner[4] refers to the individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of a CIS.

Data owner refers to the individual responsible for ensuring the protection and use of a specific data set handled by a CIS.

Requester refers to the system owner or another service requiring access to one or more CISs that submits the request to DIGIT for an external network connection.

Local Informatics Security Officer (LISO) refers to the officer who is responsible for IT security liaison for a Commission department.

User refers to any individual who uses functionality provided by a CIS, whether inside or outside the Commission.

Network service provider refers to the body within the Commission that is responsible for providing external network connection services. Generally, this is the Directorate-General for Informatics (DG DIGIT).

Interconnection security agreement (ISA) refers to a formal agreement on security measures that are required for accessing Commission information or CISs across the perimeter of the Commission's internal network.

Interconnection Security Approval Authority (ISAA) refers to the body within the Commission that is responsible for approving the security measures required for external network connections. The ISAA is in the Security Directorate of the Directorate-General for Human Resources and Security (HR.DS). This function may be delegated to another body for external connections to internal networks that are not provided by DG DIGIT, in accordance with Art. 7(4) of 2018/559[5].

Change advisory board (CAB) refers to a body including representatives of the network service provider and the ISAA that is responsible for reviewing requests for external network connections.

Third party refers, for the purposes of this document, to an external organisation with which the Commission needs to exchange information via an external network connection.

---

4 The roles of system owner, data owner, LISO and user are defined in Commission Decision C(2017) 46, Article 2.

5 The request must be made via an ARES note from the head of the requesting body and may be granted via an ARES reply from the Director of HR.DS.

4. RISKS OF EXTERNAL NETWORK CONNECTIONS

External network connections present increased risks to the Commission's networks and systems for a number of reasons, such as:

- potential lack of physical security controls over the endpoint;
- risk of malware infection due to the endpoint being connected to other equipment, networks or media;
- risk of bridging between Commission networks and other untrusted networks;
- risk of unauthorised external access to internal network resources (e.g. through session hijacking or man-in-the-middle attacks);
- risk of communications being intercepted or eavesdropping (either electronically or physically, e.g. shoulder surfing), or exfiltration of access credentials;
- risk of network discovery by unauthorised users;

These risks may lead to consequences such as:

- data leakage;
- data corruption;
- use of endpoint devices by unauthorised people;
- unavailability of the external network connection.

The risks related to external network connections should be assessed in line with Commission Decision 2017/46 and addressed through appropriate security measures as described in this decision and its implementing rules and standards. The network service provider must address the risks relating to the network access services, and system owners must take account of the risk assessment and measures applied by the network service provider.

Any assessment or evaluation of risks relating to external network connections must take account of the following aspects, as relevant:

- the confidentiality level and type of information exchanged;
- the information systems to be accessed;
- the profiles of the users (including the nature of their relationship with the Commission);
- the authentication and authorisation measures to be applied (for users and devices);
- the security measures applied to the end devices;
- the internal and external locations involved; and
- the security of the communication channels.

5. CONNECTION TYPES

External network connections are offered as shared IT services and described in the IT service catalogue. They are provided by a network service provider and are categorised into one of the following:

> **Baseline connection** – a connection that complies with the baseline security rules defined in this standard (see section 7) or with another baseline issued by HR.DS under this standard[6]. These connections are provided by the network service provider and are

[6] Security baselines for specified scenarios involving an external network connection and a use case will be established in collaboration with competent authorities where relevant (such as the Cloud Council) and need to achieve at least equivalent security to the baseline laid out in this standard.

controlled by the central security perimeter services[7] in line with this document. Baseline connections include the Commission's standard internet connections and connections between networks controlled by the network service provider, exclusively traversing segments under the control of the network service provider.

When the measures laid down for the baseline connections are implemented and included in the contracts with third parties (where relevant), an ISA is not required.

Custom connection – any other connection is considered as a custom connection, even if it is a standard service from the network service provider.

An ISA is required for each custom connection.

The classification of a connection as baseline or custom is determined by the ISAA in collaboration with the network service provider, based on an evaluation of the relevant risks.

6. INTERCONNECTION SECURITY AGREEMENT

The ISAA is responsible for providing a draft ISA for the requester to complete, and must formally approve each ISA. The CAB may be consulted for advice at the discretion of the network service provider and the ISAA.

When an ISA is required, it must be signed by all relevant parties before the connection in question is activated. The relevant parties must include the ISAA, the network service provider, the Commission department requesting the connection, the LISO of that department and any third parties that will use the connection. The ISAA must also verify that the system owner and/or data owner (as relevant) of any other Commission CIS to be accessed have also given their approval for this type of external access.

The ISA must contain a description of the connection and the service(s) using it, the Commission information or CISs that will be accessed, and the security rules that must be followed by the appropriate parties as specified.

The system owner has the responsibility for ensuring that a CIS complies with the Commission's security rules, with the support of the network service provider and other parties as necessary. Before external access is granted to a CIS, the system owner must identify, assess and treat the risks related to the external network connection. Whenever necessary, the system owner must issue detailed security requirements to be taken into account by the requesting party early in the initiation/planning phase of external network connections. The system owner must also define the authorised user population and the communication needs (network ports and protocols).

The LISO must review the request and related documentation to verify that the Commission's security rules are complied with.

The related contracts between the Commission and the external parties must include appropriate confidentiality clauses before the ISA is completed, in line with the confidentiality level of the information to be exchanged. Where relevant, third party personnel must complete and sign a non-disclosure agreement (NDA) or acceptable use policy in line with the contractual requirements.

The validity period for an ISA must not exceed 3 years, or, if sooner, the end date of the related service contract (where relevant). If the external connection is no longer required before the end

[7] For the purposes of this document, the central security perimeter services are shared IT services that are provided by DG DIGIT as the network service provider, providing security measures over connections to external networks (e.g. firewalls, gateways, proxies and intrusion detection services).

of the validity period, the requester must inform the Network Service Provider and the ISAA that the external connection is to be deactivated immediately.

If a renewal is required, the requester must present it to the ISAA at least 1 month before the existing ISA expires. Automatic renewal is not allowed.

The network service provider must have procedures in place to ensure that connections are not provided beyond the expiry of the ISA.

Any relevant call for tender and subsequent contract must indicate the requirement for an ISA to be signed. The Commission must have the right to verify at any time during its period of validity that the ISA's terms and/or the relevant security measures are being followed.

7. SECURITY MEASURES

This section lays down the security measures that must be in place for external network connections.

Baseline connections must fulfil the security requirements of sections 7.1 and 7.2 (or any other baseline issued by HR.DS under this standard) and are offered as a standard service by the network service provider.

Custom connections must fulfil the security requirements of sections 7.1 and 7.3 and an ISA must be established and signed by all relevant parties before activation. The connection must fulfil any additional security requirements specified in the ISA.

7.1. Rules for all external connections to Commission CISs

7.1.1. Governance

All external network connections must be provided under contracts managed by DG DIGIT, unless a derogation is approved by the ISAA in agreement with the Information Technology and Cybersecurity Board (ITCB). The ISAA has the right to verify the security measures for external network connections at any time, and to terminate the connection in the event of non-compliance.

The network service provider must fully document[8] security aspects of the network access service made available to system owners. The documentation must explicitly mention the level of security provided and define the key security features.

The network service provider must maintain an inventory of all external network connections and their configurations.

Contractors and other third parties must inform the Commission of any security incidents that could affect the external network connection, the Commission's internal network or any Commission CIS. This obligation must be included in contracts with third parties.

7.1.2. Network access services

Network access services[9] must be designed to take account of the assessed risks.

[8] As described in Commission Decision (EU, Euratom) 2017/46 Article 7 (9, 14).

Network access services must provide features to ensure confidentiality, integrity, accountability and non-repudiation as necessary in a way that helps uphold the principles of need-to-know and least privilege access in line with the security needs of the information to be accessed.

Network access services must restrict connections only to specified parts of CISs or networks (e.g. domains) via defined entry points.

Unauthorised external connections must be prevented. In particular, the default configuration must block all communications on security gateways that are not explicitly authorised.

All information traversing any non-Commission networks that is not categorised as 'publicly available' must be encrypted in line with the Commission's technical standards[10] or as stipulated in the ISA.

Any traffic that is initiated from external networks or devices must only go to servers located in a segregated area (e.g. virtual networks of the private cloud on premises, extranet servers, terminal servers, reverse proxies or other communication gateways), and must not directly address any other devices on the internal network. All devices that can be directly addressed must be hardened and kept up to date with security patches in line with the relevant standard[11].

All inbound and outbound traffic must be filtered and inspected, where possible[12], to detect threats such as intrusion attempts and malware, in line with the relevant technical standard[13] and the regulation on data protection[14].

All security-related events must be identified and logged to ensure accountability and support the incident response processes, and these logs must be maintained for at least 6 months.

The network service provider must have procedures to deactivate external connections or to disconnect individual users when necessary, for example under the incident handling procedure or if there is a clear threat to the Commission's network infrastructure coming via the external connection. The network service provider must also deactivate external connections immediately when so requested by the ISAA or HR.DS, for instance in the context of a security investigation.

External connections must be disconnected when no longer required.

The network service provider must systematically assess the security measures of external connections.

---

9 The term 'network access service' refers to all components involved in providing an external connection, including the communications controllers, gateways and endpoints (internal and external).

10 See the Standard on cryptography and public key infrastructure and C(2019) 2346 final IT security standard on Transport Layer Security (TLS).

11 C(2018) 7284 final IT Security Standard on IT Vulnerability and Remediation Management

12 Interception of encrypted communications may be possible or not depending on the type of connection, the information being exchanged and any relevant legal considerations. Where it is not possible, appropriate measures must be taken at the endpoint(s) of the encrypted channel.

13 C(2020) 4296 final IT security standard on Logging and monitoring

14 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21.11.2018, p. 39-98

7.1.3. Security perimeter services

The security features of the security perimeter service must be maintained in line with current best practices, including at least the following features where applicable:

- External network connections must be segregated from each other in the security perimeter service to prevent the Commission's network infrastructure from being used as a bridge to access other external networks.
- Network security zones must be defined and protected by firewalls. The rules must restrict traffic based on at least the required sources, destinations and the required network protocols. Firewall rules must be set to deny access by default and to be as restrictive as reasonably possible.
- Appropriate measures to ensure authentication, authorisation and accounting must be implemented in the security perimeter service.
- Any reverse proxy deployment for a CIS on the Commission's internal network must comply with the reverse proxy mapping policy[15].
- Any servers that are accessed via a central reverse proxy or application gateway infrastructure must be located in a network zone that is separate from the reverse proxy.

7.1.4. Authentication and session management

Passwords or other persistent authentication information must comply with the relevant Commission IT security standards and must not be stored or transmitted without encryption.

Authentication methods must be used for end user access to Commission CISs through remote access services in line with the relevant IT security standard[16], delivering at least a medium level of authentication. Authentication credentials used for external access must be deactivated as soon as they are reported lost or stolen.

A session time-out and idle time-out must be set for end user connections. The justification for any exceptions must be documented in the relevant IT security plan.

7.1.5. End devices

Security requirements for end devices must be documented and enforced by the system owner or the network service provider as appropriate before a session is opened. The use of Commission-controlled end devices is preferred where possible, to reduce the risk of changes to the security configuration.

To the extent possible, passwords must not be stored in the end user device.

7.1.6. Access to CISs

The decision on whether to allow external connections to a CIS, directly or indirectly, must be taken explicitly by the system owner, based on a risk assessment, and documented in the IT security plan.

The system owner may apply restrictions on access via external connections, such as:

[15] The reverse proxy mapping policy is a set of rules established by the network service provider that defines the accessibility of internal domains and rules for permitting access from external networks via the proxy.

[16] C(2019) 2344 final IT security standard on Access control and authentication

- the permitted user population;
- the devices that can be used;
- different roles for remote access with restricted authorisations; and
- the protocols that can be used to access the system.

To access a CIS that is outsourced, the CIS must follow the rules laid down in Article 8 of Commission Decision (EU, Euratom) 2018/559 and the Principles for outsourcing of communication and information systems[17].

7.2. Rules for baseline connections

All traffic in baseline connections must pass through a central security perimeter service located in a demilitarised zone (DMZ) in order to prevent direct connections between devices on the internal network and untrusted external networks or devices.

Remote access solutions that are terminated on a user's internal Commission workstation are not permitted.

All outgoing internet requests must be logged and filtered to block any websites that are deemed harmful to the Commission (e.g. malware, peer-to-peer networking and unauthorised remote access tools). The categories of websites to be blocked must be determined by DG HR jointly with DG DIGIT, informing the ITCB of any changes.

The connection must be protected against denial of service attacks that may jeopardise the availability of network services or CISs.

7.3. Rules for custom connections

All traffic must pass through a central security perimeter service located in a demilitarised zone (DMZ) in order to prevent direct connections between devices on the internal network and untrusted external networks or devices, unless specifically authorised[18]. The rules allowing traffic to pass must be highly restrictive, based on the sources, destinations and permitted network protocols.

Remote access solutions that are terminated on a user's internal Commission workstation are only permitted when this is specified in the ISA and appropriate security measures are implemented.

The ISA must lay down any other applicable measures, particularly in the following areas[19]:

- authentication of users and services (including revocation upon termination);
- security measures on external endpoints;
- security measures on internal endpoints;
- measures for prevention or acceptable use of network bridging;
- least privilege authorisations for end users;
- protection of data in transit (e.g. encryption of traffic);
- anti-malware controls;
- measures to prevent unauthorised use;

[17] C(2020) 4190 - Principles for outsourcing of communication and information systems, 18.6.2020

[18] Some connections may be made directly through the firewalls without passing through a proxy but these should be restricted to the minimum possible.

[19] Consult the relevant standards under Commission Decision (EU, Euratom) 2017/46 for the detailed rules on applicable security measures.

- acceptable use policies;
- logging and monitoring;
- security incident handling procedures, including the obligation to inform the other parties of any security incidents; and
- secure handling and deletion by third parties of Commission information.

8. EXTERNAL AND REMOTE USERS

Access rights for external or remote users, including privileged users, must be maintained and updated by the system owner as required by the access control policy of each CIS, including shared IT services that provide external network connections, and removed as soon as the authorisation is revoked.

System owners must consider restricting access to certain services or functions for remote users (i.e. requiring users to be present on Commission or other authorised premises), especially if they can carry out sensitive operations on Commission CISs.

Training or written guidelines must be provided to users, outlining their responsibilities and providing advice on reducing the risks of external connections, covering in particular the following issues.

- Users must be especially careful about protecting their credentials (e.g. not keeping their passwords in the same bag as their portable PC). Authentication mechanisms must be protected.
- Users must be aware of the physical security of the environment where they are using external connections and take appropriate steps to reduce risks such as eavesdropping, unauthorised observation of their activities, and loss or theft of their equipment or credentials.
- Users must not store sensitive non-classified information on non-Commission devices or services (e.g. external information-sharing platforms).
- Users must not allow unauthorised people to use the Commission's remote access services, including friends and family members.
- Users must not attempt to deactivate or circumvent any of the security measures in place.
- Users must be attentive to signs of unauthorised use of endpoint devices. They must promptly report, via the appropriate channels, any suspected or actual security incident or CIS vulnerability.

9. RASCI MATRIX

The following matrix shows the main roles that are involved in establishing external network connections, where:

R = Responsible

A = Accountable

S = Supporting

C = Consulted

I = Informed

Role / Process	Requester	System owner[20]	Data owner	LISO	ISAA	Network service provider	CAB	User
Define & document security requirements for baseline connections					A, R	C	C	
Define & document external network access service		C		C	C	A, R		I
Provide external network access service					C	A, R		
CIS security documentation[21]	I	A, R	C	C/S				
Request connection or renewal	A, R	C	C	C/S	C	C/S	C	
Draft ISA	A, R	C/S		C	C	S	C/S	
Approve ISA	R	I		R	A, R	R		
Prepare user training & guidelines		C	I	I		A, R		I
Ensure delivery of training		A, R				S		I
Coordination of ISA framework	I	I	I	I	A, R	C/S	C	
Verifying compliance	I	S	I	S	A, R	S		

[20] The system owner column refers to system owners of CISs to be accessed via an interconnection (idem for the data owner).

[21] The security documentation principally consists of the IT security plan. When a CIS is accessed externally, this should include information on the applicable security measures for access by external users.