RFC 2350

DOCUMENT INFORMATION

This document contains a description of the European Commission Cybersecurity Operations Centre in accordance with RFC 2350. It provides basic information about the European Commission Cybersecurity Operations Centre team, its channels of communication, and its roles and responsibilities based on European Decision 2017/46 (1).

1.1 DATE OF LAST UPDATE

This is version 2.00, published 2023/03/17.

1.2 DISTRIBUTION LIST FOR NOTIFICATIONS

There is no distribution list for notifications.

1.2 LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND

The current version of this CSIRT description document is available on request by sending a mail to EC-DIGIT-CSIRC@ec.europa.eu

Please make sure you are using the latest version.

1.4 AUTHENTICATING THIS DOCUMENT

This document has been signed with the EC DIGIT CSIRC PGP key.

2. CONTACT INFORMATION

2.1 NAME OF THE TEAM

Full Name	European Commission Cybersecurity Operations Centre
Short Name	EC Cybersecurity Operations Centre

2.2 ADDRESS

European Commission

DIGIT.S.2

Euro Forum (EUFO) Building

10, rue Robert Stumper

Office EUFO 04/192

L-2557 LUXEMBOURG

Grand-Duchy of Luxembourg

2.3 TIME ZONE

Europe/Brussels (GMT+0100, and GMT+0200 from April to October).

2.4 TELEPHONE NUMBER

+352 43 01 32601

2.5 FACSIMILE NUMBER

No communication by fax

2.6 OTHER TELECOMMUNICATION

Mobile phone number and Video conferencing available on request.

Members of the constituency have access to closed, secure communication and collaboration platforms.

2.7 ELECTRONIC MAIL ADDRESS

All notifications, incidents reporting, operational matters and non-operational matters can be addressed at :

EC-DIGIT-CSIRC@ec.europa.eu

This mailbox is monitored during business hours of working days.

2.8 PUBLIC KEYS AND OTHER ENCRYPTION INFORMATION

We rely on S/MIME for internal communications and PGP for exchange outside the European Institutions, Bodies and Agencies (EUIBAs).

Fingerprint	4E43 D957 69D3 457D 93D8 CCFD 9399 DF84 CF24 42A2
Location	https://openpgp.circl.lu/pks/lookup?op=get&search=0x4e43d95769d3457d93d8ccfd9399df84cf2442a2

2.9 TEAM MEMBERS

Guy Lambert is the head of the European Commission Cybersecurity Operations Centre.

Spyros Sarigiannidis is the deputy head.

The Centre is composed of more than 60 professionals.

2.10 OTHER INFORMATION

The European Commission Cybersecurity Operations Centre is member of

- TF-CSIRT, the Task Force on Computer Security Incident Response Teams;
- FIRST, the Forum of Incident Response and Security Teams.

The European Commission Cybersecurity Operations Centre is part of CERT-EU constituency and closely collaborates with CERT-EU on incidents that affects the European Commission.

CERT-EU is a trusted partner of the European Commission Cybersecurity Operations Centre and incidents affecting the European Commission should be addressed directly to CERT-EU to ensure coordination through all the European Institutions, Bodies and Agencies (EUIBAs).

2.11 POINTS OF CUSTOMER CONTACT

The preferred method for contacting the European Commission Cyber Security Operations Centre is via e-mail at EC-DIGIT-CSIRC@ec.europa.eu.

If it is not possible (or not advisable for security reasons) to use e-mail, the European Commission Cyber Security Operations Centre can be reached by telephone during regular office hours.

The European Commission Cyber Security Operations Centre hours of operation are generally restricted to regular business hours (09:00-17:00 Monday to Friday except EU public holidays).

There is an on-call 24/7 services available for constituents in case of emergency.

3. CHARTER

3.1 MISSION STATEMENT

The mission of the European Commission Cybersecurity Operations Centre is to provide the operational IT security within the European Commission by helping to detect, mitigate and respond to cyber-attacks.

The scope of our activities covers detection and response.

We value ethical integrity and collaboration with peers.

3.2 CONSTITUENCY

The European Commission Cybersecurity Operations Centre constituency is the European Commission.

We handle the incidents related to AS42848.

We operate on all communication and information systems (CISs) which are owned, procured, managed or operated by or on behalf of the Commission and all usage of those CISs by the Commission as defined in the decision 2017/46 available at (1).

3.3 SPONSORSHIP AND/OR AFFILIATION

The European Commission Cybersecurity Operations Centre is part of Cybersecurity Directorate of European Commission Directorate-General for Informatics (DIGIT S).

European Commission Cybersecurity Operations Centre is part of CERT-EU constituency and closely collaborates with them in full trust and transparency.

3.4 AUTHORITY

The European Commission Cybersecurity Operations Centre operates under the auspices of, and with the authoritydelegated by, the European Commission.

For further information on the mandate and authority of the Department of Computing Services, please refer to the COMMISSION DECISION (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission available at (1)

In this frame, European Commission Cybersecurity Operations Centre may have access to systems and data corporate wide to detect, analyse and handle computer security incidents. Such activities are performed according to the rules defined in Regulation (EC) 2018/1725 of 23 October 2018 available at (2)

4. POLICIES

4.1 TYPES OF INCIDENTS AND LEVEL OF SUPPORT

The European Commission Cybersecurity Operations Centre is authorized to address all types of computer security incidents which occur, or threaten to occur, at the European Commission.

4.2 CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

The European Commission Cybersecurity Operations Centre collaborates and shares information with CERT-EU and Security Directorate of the Directorate-General for Human Resources and Security (HR.DS).

All requests to the European Commission Cybersecurity Operations Centre are treated with due care. The European Commission Cybersecurity Operations Centre adheres to the traffic light protocol (TLP). See (3) for a description.

Sensitive messages should be tag in the subject as [TLP Color]. A similar stamp should be clearly visible in other documents, such as PDF files etc, sent to the European Commission Cybersecurity Operations Centre. If contact is through phone or video conference, the TLP classifications should be stated prior to the delivery of the information.

It is recommended to encrypt sensitive information with the PGP key mentioned above. Other encryption methods are available upon request.

4.3 COMMUNICATION AND AUTHENTICATION

The European Commission Cybersecurity Operations Centre protects sensitive information in accordance with relevant regulations and policies within the EU.

Communication security (encryption and authentication) is achieved by various means:

- S/Mime based email encryption (SECEM),
- PGP or other agreed means, depending on the sensitivity level and context.

5. SERVICES

IDENTIFY (ID)

The European Commission Cybersecurity Operations Centre produce regular and ad-hoc reporting on threat information based on information received from peers, open-source information, and closed-source information.

PROTECT (PR)

The European Commission Cybersecurity Operations proactively hunt for malicious activities that may target the European Commission.

DETECT (DE)

The European Commission Cybersecurity Operations actively develop monitoring rules, threat hunting campaigns, and analyse alerts raised by our different tools.

RESPOND (RS)

The European Commission Cybersecurity Operations conduct specialised analysis of cybersecurity incidents impacting the European Commission.

This cover incident support, coordination, gathering artifacts, digital forensics, analysis of malicious files and binaries and if required, communicating with relevant parties and authorities. The service also delivers several automated analytical tools to our constituency.

RECOVER (RC)

The European Commission Cybersecurity Operations contributes to recover from incident by producing frequent and ad-hoc reporting as well as advising based on incident lessons learned.

6. INCIDENT REPORTING FORMS

There are no forms available.

The preferred way of reporting is by email.

7. DISCLAIMERS

While every precaution will be taken in the preparation of information, notifications and alerts, the European Commission Cybersecurity Operations Centre assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.

8. SECURITY CONSIDERATIONS

This document discusses the operation of Computer Security Incident Response Teams, and the teams' interactions with their constituencies and with other organizations. It is, therefore, not directly concerned with the security of protocols, applications, or network systems themselves. It is not even concerned with particular responses and reactions to security incidents, but only with the appropriate description of the responses provided by CSIRTs.

Nonetheless, it is vital that the CSIRTs themselves operate securely, which means that they must establish secure communication channels with other teams, and with members of their constituency. They must also secure their own systems and infrastructure, to protect theinterests of their constituency and to maintain the confidentiality of the identity of victims and reporters of security incidents.

BIBLIOGRAPHY

1. **European Commission.** COMMISSION DECISION (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission. [Online] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1548167340412&uri=CELEX:32017D0046.

2. **European Parliament.** 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. [Online] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32018R1725.

3. **FIRST.org.** TRAFFIC LIGHT PROTOCOL (TLP). *FIRST Standards Definitions and Usage Guidance — Version 2.0.* [Online] https://www.first.org/tlp/.

4. **Fraser, .** *Site Security Handbook.* September 1997. FYI 8, RFC 2196.

5. **Malkin, .** *Internet Users' Glossary.* August 1996. FYI 18, RFC 1983.

6. **Brownlee, .** *Expectations for Computer Security Incident Response.* RFC2350.