Council of the European Union
General Secretariat

Brussels, 11 January 2021

CM 1022/1/21
REV 1

CYBER
COPEN
COPS
COSI
DATAPROTECT
IND
JAI
JAIEX
POLMIL
RELEX
TELECOM

COMMUNICATION

NOTICE OF MEETING AND PROVISIONAL AGENDA

Contact:	cyber@consilium.europa.eu
Tel./Fax:	+32.2.281.8570 / 7040
Subject:	Horizontal Working Party on cyber issues
Date:	12 January 2021
Time:	10.00, 15.00
Venue:	COUNCIL JUSTUS LIPSIUS BUILDING Rue de la Loi 175, 1048 BRUSSELS

Format: 1+0 (Presidency 1+1)

Please note the Council's Security Regulations outlined on page 2 and 3, including the need to register all the delegates (1 per Member State) who will participate in the classified item of the meeting - ***CONFIDENTIEL UE/EU CONFIDENTIAL*** - meaning that the presentation and following discussion will take place in a secured meeting room.

Delegations are informed that the discussion of items 1 to 6 of the agenda will take place via videoconference and will start at 10.00h.

The discussions of agenda items 7 to 12 will take place in meeting room 35.4 and will start at 15.00h.

Part 1: Videoconference starting at 10.00h

1. **Adoption of the agenda**

2. **Presentation of the Presidency Programme**

3. **The EU's Cybersecurity Strategy for the Digital Decade: Q&A**

   doc. 14133/20

4. **Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148: Q&A**

   doc. 14150/20

5. **UN Third Committee: Briefing by the EEAS and the Commission on latest developments in the field of cybercrime**

6. **AOB**

Part 2: Physical meeting starting at 15.00h (Room JL 35.4)

7. **Elements for draft Common Lines To Take on Data Security: Presentation by the EEAS**

   doc. EEAS 2020/1423 (RESTREINT UE/EU RESTRICTED)

8. **Cyber-enabled IP Theft: Presentation by Intcen**

9. **COVID-19 related cyber threats: Presentation by INTCEN & CERT-EU**

10. **Other cyber threats: Presentation by INTCEN & CERT-EU**

11. **Cyber diplomacy toolbox related discussion**

12. **AOB**

* * *

Note:** This meeting will cover information classified ***CONFIDENTIEL UE/EU CONFIDENTIAL please see **items 8-11** of the agenda. In accordance with the Council's security rules, all delegates present at the discussion of such items must have a **valid personnel security clearance for access to EU classified information at least up to *CONFIDENTIEL UE/EU CONFIDENTIAL* level**.

A maximum of 1 participant per delegation can attend.

Delegates should note that in accordance with the Council's Security Rules, only persons with a need-to-know may be admitted to meetings where classified information is to be discussed.

List of participants

Delegations are requested to forward to **WP-CYBER@consilium.europa.eu by 08 January 2021 17:00 (Brussels time)** the following details for the delegate taking part in the discussion of these items: **full surname(s), given name, nationality, date of birth** and name of the organisation/institution sending him/her to the meeting.

Personnel Security Clearance

In accordance with the Council Decision on the Security Rules for Protecting EU Classified Information (2013/488/EU), all delegates attending those meetings must be in possession of a valid EU security clearance up to the level CONFIDENTIEL UE/EU CONFIDENTIAL.

No admission to the discussion of this item will be granted to delegates for whose clearances the GSC Safety and Security Directorate has no record or who cannot present a valid, original personnel security clearance certificate issued by their National Security Authorities or by other competent national authorities.

Only in case **a Personnel Security Clearance Certificate for the delegate concerned has not yet been transmitted to the Security Office, a copy should be sent by National Security Authority** or other competent national authority or your **organisation's security officer to the following email address, also by 08 January 2021 17:00 (Brussels time)**
security.clearances@consilium.europa.eu

It is in the interest of the participants to ensure that their personnel security clearance has not expired.

Please note that certificates sent by the delegates themselves will not be accepted.

During the discussion of CONFIDENTIEL UE/EU CONFIDENTIAL items, all electronic devices must be switched off.

NB: Council documents are available on Delegates Portal. Room attendants will provide copies on request at the earliest opportunity.

NB: Please send a list of your delegates to this meeting as soon as possible to the email address access.general@consilium.europa.eu