



Brussels, 19 March 2021

CM 2343/21

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: +32.2.281.5397 / 7040

Subject: Informal VTC of the Members of the Horizontal Working Party on cyber issues (morning 10:00 - 13:00)

Horizontal Working Party on cyber issues (afternoon, 14:30)

Date: 24 March 2021

Time: 10.00

Venue: COUNCIL

JUSTUS LIPSIUS BUILDING

Rue de la Loi 175, 1048 BRUSSELS

Morning session starting at 10h00 (VTC)

1. Adoption of the agenda
2. 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: read-through of Articles 18 to 23 followed by Q&A

- doc. 14150/20 and ADDs

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

3. EU Cyber Diplomacy Toolbox (*CONFIDENTIEL UE/EU CONFIDENTIAL*)

- Continuation of the discussions from the HWPCI meeting of 22 March 2021 (poss.)
doc. EEAS 10091/21 (*CONFIDENTIEL UE/EU CONFIDENTIAL*)

- Continuation of the discussions from the HWPCI meeting of 12 January 2021

4. EU – Africa Cybersecurity: Presentation by INTCEN (*CONFIDENTIEL UE/EU CONFIDENTIAL*)

5. Annual review of the designations under restrictive measures: Presentation by the EEAS followed by discussion with a view to approval (*CONFIDENTIEL UE/EU CONFIDENTIAL*)

6. Draft EU Lines to Take in view of the seventh meeting of the UN IEG on cybercrime:
Presentation by the EEAS and Commission followed by discussion with a view to approval
doc. 7178/21

7. Cyber elements of the EU Integrated Resolve: Presentation by the EEAS

8. AOB

* * *

***Note:** This meeting will cover information classified *CONFIDENTIEL UE/EU CONFIDENTIAL*, please see **items 3, 4 and 5** 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**. Due to the high classification level, items 3, 4 and 5 will take part in the secured meeting room.

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 **19 March 2021** **COB** the following details for each 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 them 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 19 March 2021 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