Council of the European Union

**Brussels, 22 March 2022**
**(OR. en)**

**7474/22**
**ADD 3**

**Interinstitutional File:**
**2022/0085(COD)**

**CYBER 93**
**TELECOM 116**
**JAI 383**
**INST 89**
**INF 32**
**CSC 119**
**CSCI 39**
**DATAPROTECT 81**
**FIN 353**
**BUDGET 2**
**CODEC 349**
**IA 30**

**COVER NOTE**

| | |
|---|---|
| From: | Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director |
| date of receipt: | 22 March 2022 |
| To: | Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union |
| No. Cion doc.: | SWD(2022) 68 final |
| Subject: | COMMISSION STAFF WORKING DOCUMENT<br>SUMMARY OF THE IMPACT ANALYSIS Accompanying the document Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union |

Delegations will find attached document SWD(2022) 68 final.

Encl.: SWD(2022) 68 final

EUROPEAN
COMMISSION

Brussels, 22.3.2022
SWD(2022) 68 final

**COMMISSION STAFF WORKING DOCUMENT**

**SUMMARY OF THE IMPACT ANALYSIS**

***Accompanying the document***

**Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

**laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union**

{COM(2022) 122 final} - {SWD(2022) 67 final}

## 1. Introduction

In 2020, the number of significant incidents affecting Union institutions, bodies and agencies, authored by advanced persistent threat (APT) actors, surged. This is also reflected in the number of forensics images CERT-EU analysed in 2020, which more than tripled in comparison to 2019, while the number of significant incidents rose more than tenfold since 2018.

However, the cybersecurity capabilities and IT security spending in the Union institutions, bodies and agencies are in some cases strikingly unequal, resulting in a broad spectrum of cybersecurity maturity levels between the Union institutions, bodies and agencies. Additionally, the threat landscape analysis and IT security incident statistics show that cyber exposure for Union institutions, bodies and agencies will only intensify.

## 2. Objectives

The shortcomings identified, ultimately lead to an insufficient level of cyber resilience across the Union institutions, bodies and agencies, fragmented IT security resourcing and unbalanced IT security postures.

The aim of a legislative act would be to provide measures for a high common level of cybersecurity at the Union institutions, bodies and agencies. This would foster and assure that the cybersecurity maturity will keep pace with the accelerating digitalisation of Union institutions, bodies and agencies.

## 3. An Interinstitutional Cybersecurity Board and a cybersecurity framework

The proposal of an Interinstitutional Cybersecurity Board and a cybersecurity framework will introduce measures for a high common level of cybersecurity at the Union institutions, bodies and agencies enabling alignment around a framework that addresses the cybersecurity threats of all the Union institutions, bodies and agencies and will establish monitoring and reporting to an Interinstitutional Cybersecurity Board.

The proposal modernises CERT-EU's mission and tasks considering the changed and increased digitisation of the Union institutions, bodies and agencies in recent years and the evolving cybersecurity threat landscape.

There are no direct impact or budgetary consequences for the Member States or EU citizens.

The legal ground for the Regulation is Article 298 of the Treaty on the Functioning of the European Union which foresees that in carrying out their missions, the institutions, bodies, offices and agencies of the Union shall have the support of an open, efficient and independent European administration.

This proposal builds on the EU Security Union Strategy (COM(2020) 605 final) and the EU's Cybersecurity Strategy for the Digital Decade (JOIN(2020) 18 final).

## 4. Conclusion

An Interinstitutional Cybersecurity Board and a cybersecurity framework achieves most of the intended objectives in a relatively effective, efficient and coherent manner with other Union policies with the broadest stakeholders support. This solution that has been selected is the most viable option given the prevailing legal boundaries under which we act, also, a 'one-size fits all' approach would not respond to the heterogeneous maturity of the Union institutions, bodies and agencies today and disparities in technological risk and complexity that they face.