REPLIES OF THE EUROPEAN COMMISSION

TO THE EUROPEAN COURT OF AUDITORS' SPECIAL REPORT

Cybersecurity of EU institutions, bodies and agencies: Level of preparedness overall not commensurate with the threats

Contents

This document presents the replies of the European Commission to observations of a special report of the European Court of Auditors, in line with Article 259 of the Financial Regulation and to be published together with the Special Report.

I. THE COMMISSION REPLIES IN BRIEF

a) General introduction

Cybersecurity has become a top political and operational priority of the European Commission. The COVID crisis has accelerated our dependence on digital services (cloud computing, mobile devices, artificial intelligence). In the past two years, we have seen a massive shift towards working from home. This means that both cyber criminality and cyber espionage, the two main threats facing the EUIBAs (European Union Institutions, Bodies and Agencies), have effectively also gone online in a big way. The Commission recognises this trend. It has shown consistent and decisive leadership on cybersecurity. The Cybersecurity Act came into force in 2019, inter alia expanding the mandate of ENISA and putting it on a permanent footing. This Act also established a formal cooperation between ENISA and CERT-EU (the computer emergency response team supporting all the EUIBAs). In 2020, the Commission proposed a reinforcement of the Network and Information Security Directive, which is close to agreement in the legislature.

The 2020 Cybersecurity Strategy also contained three actions bearing on the cybersecurity of the EUIBAs. It announced a Regulation on Information Security in the EU institutions bodies and agencies, a Regulation on Common Cybersecurity Rules for EU institutions, bodies and agencies and its intention to provide a new legal base for CERT-EU to reinforce its mandate and funding to ensure its adequate resourcing in face of rising threats, risks and incidents.

The work of preparing these proposals has advanced. Although they are not yet adopted by the College, it is expected that they will be adopted in the first quarter of 2022. Important questions discussed between the institutions at this preparatory stage concern the legal base of the proposal as well as the budgetary capacity of all EUIBAs to meet the requirements both in terms of financing their own cybersecurity needs and to find the necessary resources to support CERT-EU, budget and in particular posts.

The level of cybersecurity preparedness of EU institutions, bodies and agencies has varying levels of maturity. Several EUBIAs do have a strong performance in terms of cyber preparedness and should continue to serve as leaders, stimulating and inspiring progress and further improvements across the entire cybersecurity landscape. In order to achieve measurable progress, it is important to acknowledge the varying levels of maturity among the EUIBAs and set priorities by directing the improvement actions in the first place towards those EUIBAs where the identified gaps lead to the highest risk exposure.

b) The Commission's position on the key ECA observations and recommendations

The Commission welcomes the ECA's report on Cybersecurity of EU institutions, bodies and agencies. It takes note that the report underlines the importance of common legal frameworks for all EUIBAs on information security and cybersecurity to increase the overall level of cybersecurity across the board. The Commission notes that the main observations and recommendations of the ECA are not targeted at the Commission's own operational cybersecurity per se, but at the Commission's policy role in proposing legislation to raise the cyber maturity of the EUIBAs.

The future Regulations on 'Information Security in the EU institutions bodies and agencies' and 'Common Cybersecurity Rules for EU institutions, bodies and agencies' will set the common rules towards achieving high levels of information security and cybersecurity but their implementation, within the organisational and operational context of each EUIBA (in particular, their threat and risk profiles), remains under the autonomous responsibility of the EUIBAs. The proposed Regulation on cybersecurity will have compliance mechanisms that are appropriate and commensurate to the objective and scope of the new rules, without prejudice to the autonomy of institutions, bodies and agencies.

The Commission currently chairs the cybersecurity sub-group of the inter-institutional committee on digital transformation (ICDT) which is a rotating appointment (for the period of up to 2 years). It is noted that no dedicated resources given to the work of the sub-group: all actions are based on best efforts by the participants on a voluntary basis.

The Commission agrees with the general idea of reinforcing CERT-EU's resources and mandate.

With this understanding, the Commission supports the key observations and recommendations of the report. Our detailed position is explained in the additional comments in section III. Regarding the recommendations, the Commission accepts recommendations 1a, b, c, d, e, f, g and 2a, b, c.

c) Relevant latest developments and next steps

A formal consultation at the level of Directors-General of EUIBAs on the consolidated drafts of the two Regulations (information security, cybersecurity) has been completed and the assessment of the received feedback is ongoing, prior to completion of the package and adoption by the College in the first quarter of 2022.

II. COMMISSION REPLIES TO MAIN OBSERVATIONS OF THE ECA

1. Cybersecurity maturity levels of EUIBAs

The Commission agrees that when observing the level of spending by EUIBAs on cybersecurity it is important to take into account threats and risks.

Similarly, with regards to the human resources aspect, the stability of EUIBA staffing is influenced by a number of factors. The market for the recruitment of specialized cybersecurity experts is increasingly complex. In many cases, human resources rules are not adapted to specialised profiles (recruitment, career development, training). Moreover, the generalized pressure on staffing levels across the EUIBAs by the budgetary authority means that emerging areas of high priority such as cybersecurity remain under-supplied by posts, notably in internal operational services.

The reference to progress on governance and risk management should take into account the fact that the monitoring of compliance is now moving from pilot to full roll-out. Thus, it is normal that the coverage is so far quite low. This compliance project is the next stage of a long-term cyber maturity improvement process that began with the definition of a common risk methodology, the construction of common tooling, the rollout of vulnerability management and asset inventory monitoring, testing and validation. Progress has been made along this long path despite the

complexity of the Commission's asset base with more than 1 000 information systems operated by more than 50 Directorates-General and Executive Agencies.

2. EUIBAs mechanisms for cooperation

CERT-EU is a phenomenal success story in promoting cooperation not only between EUIBAs, but also at European level, through its participation as a full member of the CSIRT network set up under the NIS Directive. In this way, CERT-EU is an exemplary case of how cooperation and cybersecurity services can be enhanced. The ECA's observations on CERT-EU illustrate very clearly the outstanding job that CERT-EU is doing in the face of an increasingly hostile cyber threat landscape and with chronic under- resourcing.

Under the present Interinstitutional Arrangement (IIA), EU decentralised agencies and joint undertakings are officially represented in the CERT-EU steering board by ENISA. Beyond that, their views are voiced in steering board meetings by an ICT Advisory Committee (ICTAC) representative, who is permitted to attend to assist ENISA in its role of representing the agencies but has no formal seat or vote. The point of adequate representation of agencies in the CERT-EU steering board will be addressed in the proposed Regulation by completing the composition of the steering board with up to three representatives designated by the Union Agencies Network (EUAN), upon a proposal by its ICT Advisory Committee.

Participation in the cybersecurity sub-group of the ICDT is on a best effort basis, at the level of engagement decided by each EUIBA. Improvements on information sharing on procurement, as an important subject within the scope of Task Force 2 of the Cybersecurity Subgroup, are being addressed in the preparation of the new cybersecurity framework contract.

Regarding common tooling for services such as email and videoconference, there is already the facility to use SECEM-2 system implemented by the Commission for all the EUIBAs, for encrypted email depending on the effective management of encryption keys and certificates. Adding to that, SECABC, a tool to enable email encryption between institutions is under development, with the intention to offer access to it to every interested EUIBA as from 2022. Secure videoconferencing for SNC services is already achieved and can be extended to other EUIBAs on an ad hoc basis by managing the identities of the participants in the meeting. Sharing of sensitive information will also be addressed in the proposed Regulation on information security (i.e. through common labelling and markings).

3. Sharing information about significant incidents or vulnerabilities

The fact that not all EUIBAs are notifying CERT-EU of significant incidents or vulnerabilities is addressed in the draft cybersecurity Regulation in line with the Commission's proposal in the NIS-2 Directive[1]. The level of implementation will depend on extra resources dedicated to this by the autonomous EUIBAs. The scope for enforcement of such notifications remains limited, including under the proposed Regulation as currently planned, due to the institutional autonomy of the EUIBAs. The proposed Regulation on cybersecurity will have compliance mechanisms that are

[1] 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, COM/2020/823 final

appropriate and commensurate to the objective and scope of the new rules, without prejudice to the autonomy of institutions, bodies and agencies.

III. COMMISSION REPLIES TO THE CONCLUSIONS AND RECOMMENDATIONS OF THE ECA

Recommendation 1 – Improve the cybersecurity preparedness of all EUIBAs through common binding rules and increased resources for CERT-EU

The proposed text of the Regulation will include specific measures designed to further increase the common level of cybersecurity. Said measures will be translated into cybersecurity plans, defined and implemented at the level of the EUIBAs under their own cybersecurity governance framework.

The Commission accepts this recommendation. With reference to the specific sub-recommendations, the Commission notes the following:

a) The Commission accepts recommendation 1a. The draft Regulation will include provisions on governance and control frameworks, set up at the highest level of executive management of each EUIBA, to ensure an effective and prudent management of all cybersecurity risks.
b) The Commission accepts recommendation 1b. The draft Regulation will reinforce the mention of the risk-based approach to managing cybersecurity by making it clear that actions, IT security plans and actual implementation of essential controls should follow the assessments.
c) The Commission accepts recommendation 1c. Cybersecurity education, awareness-raising and training programmes will be cited as a part of the cybersecurity baseline in the draft Regulation.
d) The Commission accepts recommendation 1d. In our experience, although regular audits and tests are essential, they are not sufficient to make sure that progress is being made. Thus, regular reporting and transparency is necessary, as a part of cybersecurity governance framework under item a).
e) The Commission accepts recommendation 1e. The draft Regulation will include provisions related to notification, by the EUIBAs, of significant cyber threats, vulnerabilities and incidents to CERT-EU.
f) The Commission accepts recommendation 1f. The Commission supports the need to reinforce the resources of CERT-EU. Provisions related to staffing and financial contributions from the EUIBAs will be included in the text of the draft Regulation.
g) The Commission accepts recommendation 1g. The proposed Regulation will have compliance mechanisms that are commensurate and proportionate to the objective and scope of the provisions, in the respect of institutional autonomy of EUIBAs. The content of the future Regulation depends on the outcome of the legislative procedure and is the result

of a decision made by the EU Legislator with respect to the proposal made by the Commission.

Recommendation 2 - Advocate for further synergies among EUIBAs in selected areas

The Commission, currently chairing the Cybersecurity Subgroup of the Inter-institutional Committee on Digital Transformation (ICDT), agrees with the recommendations to promote the solutions for consistent and secure sharing of sensitive information, the systematic sharing of information on cybersecurity projects and common procurement frameworks and contracts for cybersecurity services.

The Commission accepts this recommendation. With reference to the specific sub-recommendations, the Commission notes the following:

a) The Commission accepts recommendation 2a. The Commission is bringing technical initiatives and services to the ICDT Cybersecurity Subgroup to promote and support common tooling for sharing of sensitive information, enabling the services such as email and videoconference. We also note that common markings and common handling rules for sensitive non-classified information will be addressed in the proposed Regulation on information security.
b) The Commission accepts recommendation 2b. The existing task forces under the ICDT Cybersecurity Subgroup is addressing this point and it will be developed further. Improvements on information sharing on procurement are being addressed in the preparation of the new cybersecurity framework contract.
c) The Commission accepts recommendation 2c. EUIBAs already have access to inter-institutional framework contracts in the area of ICT managed by the Commission. The preparation of the new cybersecurity framework contract will be coordinated with the ICDT Cybersecurity Subgroup.

Recommendation 3 - Increase CERT-EU's and ENISA's focus on less mature EUIBAs

This recommendation is addressed to CERT-EU and ENISA.