Replies of the Chair of CERT-EU's Steering Board, CERT-EU and ENISA to the European Court of Auditors' special report on the cybersecurity of EU institutions, bodies and agencies

1. Executive summary

In the light of the continuously evolving cyber threat landscape, cybersecurity has become of utmost importance and criticality for EUIBAs, which have been increasingly targeted by highly sophisticated cyberattacks over the last years. In the framework of their mandates, ENISA and CERT-EU can both provide valuable support to EUIBAs on cybersecurity at different levels. The European Commission's proposal for a Regulation on measures for a high common level of cybersecurity at the EU institutions, bodies and agencies is a key instrument in this context, an instrument which ENISA, CERT-EU and the Chair of CERT-EU's Steering Board strongly support.

To this end, ENISA, CERT-EU and the Chair of CERT-EU's Steering Board welcome the European Court of Auditors' special report on the cybersecurity of EU institutions, bodies and agencies, which comes at a very timely moment to address the level of preparedness of EUIBAs as a whole. The report clearly notes the central roles that ENISA and CERT-EU can play in this field. It also outlines the needs for further resources and concrete actions specifically targeted towards improving the cybersecurity posture of EUIBAs.

With this understanding, ENISA, CERT-EU and the Chair of CERT-EU's Steering Board support the key observations and recommendations of the report, which are also aligned with the European Commission's legislative proposals in the areas of cybersecurity and information security for EUIBAs.

The comments in the next section aim to give some further clarifications to certain areas of the report, in particular as regards relevant work already undertaken by ENISA and/or CERT-EU, as well as the envisaged actions that ENISA and/or CERT-EU have foreseen, especially in the areas of capacity building for EUIBAs. Regarding the recommendations, ENISA and CERT-EU accept Recommendation 3 (Increase CERT-EU's and ENISA's focus on less mature EUIBAs), which is specifically addressed to these two entities.

2. Main observations

ENISA and CERT-EU support the key observations established by the Court of Auditors. That being said, some additional clarifications are provided below, especially as regards the existing undertaken actions by ENISA and/or CERT-EU, as well as plans which have been already established for future activities.

Paragraph 49

Regarding the formal request sent by ICTAC to the Chair of the CERT-EU's Steering Board for voting rights on the board, we would like to clarify the following:

Given the considerable overhead that reviewing the current IIA would have entailed and because ongoing works on the "Regulation on measures for a high common level of cybersecurity at the Union institutions, bodies and agencies" had already addressed the representation of decentralised agencies, it was agreed to formally settle the matter, in a long-term perspective, through the regulation. Until then, as confirmed by the Chair, current practices will continue and ICTAC representatives will still be welcome to voice their views and have their views taken into account, to the best extent possible and in all fairness.

Paragraph 66

At the end of 2021, ENISA established an action plan for cyber-exercises, which specifically includes EUIBAs. A relevant action plan for trainings for EUIBAs will be provided in Q1 2022.

Box 3

While not explicitly mentioned as operational outputs, ENISA has been providing operational support to and co-operated with various EUIBAs based on their requests. For example, in 2018, Under Objective 2.2. Supporting European Union policy implementation:

- The European Central Bank requested support in developing the EUROSystem red team testing framework.
- The European Union Aviation Safety Agency requested support in developing the objectives of the European Centre for Cybersecurity in Aviation, in raising cybersecurity awareness and in the sectorial implementation of the NIS Directive.

- The European Union Agency for Railways requested support in NISD implementation for the rail sector, especially support in the development of a sectorial information sharing and analysis centre (ISAC) for infrastructure managers and railway undertakings, as well as capacity building (organising training and awareness-raising sessions).
- ENISA supported the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) in its efforts to better enhance its proficiency in cybersecurity and business continuity. In particular, ENISA provided its expertise in exercise organisation and scenario development, as well as offering the fully-developed ENISA CEP to eu-LISA in order to organise a preparedness exercise for one of the vital IT systems of the European Union.

Further to that, ENISA, since 2019, has been actively engaging with EUIBAs (e.g. ERA, EMSA, EASA, ACER), in support of NIS Directive, on sector-specific knowledge building and cybersecurity awareness raising activities, as well as related sectoral cybersecurity policy initiatives.

Paragraph 71

ENISA has developed in 2021 and will release in 2022 a specialised training on "How to Build an Awareness Program & Using table Top Exercises" aiming specifically EUIBAs. In the context of their structured cooperation, ENISA and CERT-EU will also provide joint trainings to EUIBAs within 2022.

Paragraph 72

It should be noted that the ENISA cybersecurity exercises have a broad scope and a wide audience, including also EUIBAs. This approach corresponds to addressing also EUIBAs needs, as EUIBAs can greatly benefit from such exercises with Member States representatives. It is noteworthy that ENISA has been involving EUIBA's technical staff as players in Cyber Europe Exercises since 2016, under the guidance of CERT-EU who is the dedicated planner of this constituency. As a continuation of these efforts, ENISA plans in its 2022 Exercise Strategy under Capacity Building Activities to promote a new exercise product that will be provided with the support of CERT EU, to give opportunities for EUIBAs to be trained in Self Evaluation Exercises.

3. Conclusions and recommendations

ENISA and CERT-EU accept Recommendation 3 (Increase CERT-EU's and ENISA's focus on less mature EUIBAs), which is specifically addressed to these two entities.