ENISA's reply to ECA's special report "Detecting and responding to cybersecurity incidents"

ENISA's reply to Recommendation 1:

ENISA accepts this recommendation whereby it shall support the Commission in implementing these recommended actions with the understanding that these additional tasks are included in ENISA's revised mandate (and in particular in its annual programming document) and subsequently supported by adequate human and financial resources.

Moreover, ENISA would also like to highlight that it is responsible for, and is developing the single reporting platform as established in the Cybersecurity Resilience Act. In the future, the Agency may be potentially tasked with the development of the single entry platform as per the "2025 digital omnibus proposal". Additionally, the Agency has also fulfilled a supportive role for the member states regarding incident reporting under the NIS2 directive. These legislative tasks are welcomed by the Agency in its role to support member states and facilitate information sharing in the European cybersecurity framework. ENISA currently has no mandate or legal role to act as incident responder whereas this competence lies within the national cybersecurity agencies / competent local authorities.

ENISA's reply to Recommendation 2:

ENISA accepts this recommendation while understanding that accountability of each party and allocated resources shall be explicitly agreed upon.

ENISA's reply to Recommendation 3:

ENISA accepts this recommendation. Moreover, whereas the Cyber Solidarity Act aims to enhance cross-border solidarity, ensuring that EU nations can assist each other in case of large-scale cyber incidents, it is important to highlight that this legislative framework does not clearly establish the nature and the scope of the cooperation between the cross-border cyber hubs and ENISA. While understanding the importance of interoperability standards to ensure effective information sharing among cross-border hubs, ENISA's restriction of not being part of the cross-border cyber hub

network resolutely reduces efficient information sharing. Therefore, ENISA does not receive or exchange information from this network and consequently is limited in adding value to enhance cross-border solidarity. In order for ENISA to efficiently facilitate this information sharing at EU level, the existing regulatory framework should therefore be amended.

ENISA's reply to Box 1. - Page 17

ENISA wishes to clarify that due to the continued absence of an agreed definition and/or guidelines of "significant incident", no member state treated this incident as being either significant or a large-scale cross-border. This case illustrates the needs to harmonize a common understanding on what constitutes a "significant incident" and subsequently to support the coordinated management of the incident.