E U R O P E A N E C O N O M I C A R E A

S T A N D I N G C O M M I T T E E
O F T H E E F T A S T A T E S

Ref. 17-4508

6 June 2018

SUBCOMMITTEE II ON FREE MOVEMENT OF CAPITAL AND SERVICES

EEA EFTA COMMENT

on the proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") (COM(2017) 477 final)

1. EXECUTIVE SUMMARY

- The EEA EFTA States welcome and support the Commission proposal to reinforce the role of the European Network and Information Security Agency (ENISA) and to give it a permanent mandate, and to establish a cybersecurity certification framework.

- The EEA EFTA States are of the view that new Regulation must respect the sovereign rights and responsibility of the members of the EEA to decide on national cybersecurity measures.

- The EEA EFTA States request clarification on several issues concerning ENISA's mandate and the system for the cybersecurity certification framework.

- The EEA EFTA States are of the view that the New Approach Notified and Designated Organisations (NANDO) Information System could be used for the listing of the notified conformity assessment bodies, pursuant to Art. 52(2).

2. INTRODUCTION

1. Through the EEA Agreement, the EEA EFTA States have participated in ENISA since 2005. ENISA has played a key role in enhancing the cybersecurity prevention work in the European Economic Area (EEA), in particular when it comes to promoting

cooperation among the member states and sharing its expertise on network information security challenges.

2. Significant changes have occurred in the cybersecurity landscape since the last revision of the ENISA Regulation was published in 2013. Therefore, the EEA EFTA States welcome and support the Commission proposal to reinforce the role of ENISA and to give it a permanent mandate, and to establish a cybersecurity certification framework. In this regard, the EEA EFTA States would like to raise their concerns about the issues that follow.

3. ENISA'S COMPETENCE VIS-À-VIS NATIONAL AUTHORITIES

3. The EEA EFTA States are of the view that there is a need to clarify in the draft Regulation how much authority ENISA will have to intervene in matters vis-à-vis national authorities.

4. There is also a need to look further into the details of what kind of operational capacity ENISA will have, as well as the type of operational assistance ENISA can provide for handling so-called "cross-border cyber crises".

5. The EEA EFTA States would like to emphasise that a new Regulation must respect the sovereign rights and responsibility of the members of the EEA to decide on national cybersecurity measures. Any extension of ENISA's mandate should not substitute this national competence.

4. THE CYBERSECURITY CERTIFICATION FRAMEWORK

6. The Commission proposal creates a system for the establishment of specific cybersecurity certification schemes for specific ICT products and services, which would allow certificates issued under those schemes to be valid and recognised across the EEA. The EEA EFTA States would like further clarification on the following issues:

   a. We recognise the rationale for only one national certification supervisory authority in each member state. The scope of the authority's responsibility will however seemingly become quite wide. In order to get the most out of existing organisations, resources and expertise, would it be possible within the regulation to split up or delegate the tasks according to Article 50(6) to other public organisations?

   b. Whether the certification framework would also relate to existing certification schemes such as the Common Criteria Recognition Agreement (CCRA) and Senior Officials Group Information Systems Security (SOG-IS), and what are the effects of the certification framework on existing certification systems such as the CCRA and SOG-IS?

7. Pursuant to Article 52 (2), notified conformity assessment bodies have to be published in the EU Official Journal. Notification is an act whereby a Member State informs the Commission and the other Member States that a body, which fulfils the relevant

requirements, has been designated to carry out conformity assessment according to a directive. Notification of notified bodies and their withdrawal are the responsibility of the notifying Member State. The EEA EFTA States are of the view that the NANDO Information System could be used for the listing of the notified conformity assessment bodies, due to a better overview and easier updating.