Three interesting features of the proposed EU Cyber Solidarity Act

EU Law analysis: Mark Young, partner, Paul Maynard, associate, and Anna Sophia Oberschelp de Meneses, associate, at Covington, consider the European Commission's proposal for an EU Cyber Solidarity Act (CSA) and set out three striking features of the CSA that are likely to be of particular relevance to private companies.

This analysis was republished on Lexis®PSL on 10/05/2023 and can be found here (subscription required)

On 18 April 2023, the European Commission published its proposal for an EU CSA. It aims to strengthen incident detection, situational awareness, and response capabilities, and to ensure that entities providing services critical for day-to-day life can access expert support to manage their cyber risk and respond to incidents. Specifically, the CSA aims to promote information sharing about cyber incidents and vulnerabilities, to help improve the cyber resilience of critical entities, and to create an EU-wide resource for incident management.

The CSA adds another layer to the increasingly crowded landscape of EU cybersecurity laws. The proposed law would interact with the revised Network and Information Security Directive, Directive (EU) 2022/2555 (NIS2) and certifications issued under the Cybersecurity Act. Private companies in specific sectors will also have to consider potential overlap with the forthcoming Cyber Resilience Act and the financial services-focused Digital Operation Resilience Act.

Below, we set out three striking features of the CSA that are likely to be of particular relevance to private companies.

Promoting platforms for information sharing and analysis

The CSA will promote the establishment and deployment of Cross-border Security Operations Centres (Cross-border SOCs), which will serve as platforms for the exchange of information and development of cybersecurity tools.

Cross-Border SOCs will be hubs for the collection and analysis of information on cybersecurity threats, incidents and tools from public bodies and private entities. Ultimately, the CSA aims to establish a 'European Cyber Shield,' comprising of several interoperating Cross-Border SOCs, each of which in turn will group together several Member State SOCs.

Importantly, the CSA does not require private entities to share threat or vulnerability intelligence with the SOCs. However, NIS2 requires Member States to facilitate voluntary information sharing, and it remains to be seen how the CSA will intersect with these requirements.

Testing certain entities that are subject to NIS2 for potential vulnerabilities based on EU risk assessments

The CSA establishes a 'Cyber Emergency Mechanism', with the aim of improving cyber resilience against major cyber threats. Article 11 of the CSA requires the European Commission to select certain industry sectors or sub-sectors that are 'highly critical'—these sectors or sub-sectors will be selected from the list in Annex 1 of NIS2, ie, sectors that comprise 'essential entities' under NIS2.

Entities in these sectors will be subject to 'coordinated preparedness testing' to examine their exposure to significant cyber threats. The NIS Cooperation Group will develop the methodology for this test, taking into account existing EU-wide risk assessments.

Requiring private providers of managed security services to support Member States in the response and immediate recovery actions in cases of significant or large-scale cybersecurity incidents

The CSA also establishes, and requires the European Commission to populate, an 'EU Cybersecurity Reserve,' comprising a bench of 'trusted providers' of private managed security services. We

understand from a Commission Q&A on the CSA that the European Union Agency for Cybersecurity (ENISA) will draw up an inventory of the services needed within the EU Cybersecurity Reserve.

Member States' Computer Security Incident Response Teams (CSIRTs) and crisis management authorities are obliged to make use of these providers' services when they assist in the management of and recovery from significant or large-scale cyber incidents affecting entities regulated under NIS2. In addition, third countries that receive funding under the Digital Europe Programme can request assistance from the EU Cybersecurity Reserve.

The CSA sets out the criteria for the selection of these trusted providers, including:

- the need to ensure that the EU Cybersecurity Reserve can provide support across all EU Member States
- the need to ensure the 'essential security interests' of the EU and the Member States
- security clearance for personnel involved in providing services
- appropriate hardware, software, and technical expertise
- once a certification scheme for managed security services under the EU Cybersecurity Act has been finalised, certification to that scheme

The requirements for trusted providers (in particular the requirements to be able to 'ensure the protection of the essential security interests' of the EU and Member States, and to obtain a certification approved under the EU Cybersecurity Act) do not explicitly exclude non-EU providers—or providers subject to non-EU legal regimes—from becoming part of the EU Cybersecurity Reserve.

Stakeholders will need to pay close attention to the details, however. Recent reports indicate that certain EU authorities are pushing to include 'sovereignty' requirements in a proposed certification scheme for cloud service providers, including requirements to ensure that non-EU government authorities cannot lawfully obtain access to data stored by cloud providers. A certification scheme for managed security providers could contain similar requirements. Equally, the Commission could interpret the requirement for providers to ensure the protection of essential security interests to mean that certain providers should be excluded, if they that could be the subject of non-EU legal process for information they hold about EU critical entities.

This article by Mark Young, Paul Maynard and Anna Sophia Oberschelp de Meneses of Covington of first appeared on 29 April 2023 on the Covington Blogs site and is republished with permission.

FREE TRIAL

The Future of Law. Since 1818.

RELX (UK) Limited, trading as LexisNexis®. Registered office 1-3 Strand London WC2N 5JR. Registered in England number 2746621. VAT Registered No. GB 730 8595 20. LexisNexis and the Knowledge Burst logo are registered trademarks of RELX Inc. © 2018 LexisNexis SA -0120-048. Reproduction, copying or extracting by any means of the whole or part of this publication must not be undertaken without the written permission of the publishers. This publication is current as of the publish date above and It is intended to be a general guide and cannot be a substitute for professional advice. Neither the authors nor the publishers accept any responsibility for loss occasioned to any person acting or refraining from acting as a result of material contained in this publication.