COVINGTON

The EU Gets Serious About Cyber: The EU Cybersecurity Act and Other Elements of the "Cyber Package"

September 18, 2017

Cybersecurity

Last week, in his annual State of the European Union Address, the President of the European Commission Jean-Claude Juncker called out cybersecurity as a key priority for the European Union in the year ahead. In terms of ranking those priorities, President Juncker placed tackling cyber threats just one place below the EU leading the fight against climate change, and one above migration and protecting Europe's external borders.

The full extent of the Commission's ambition and plans in relation to cybersecurity is revealed in a detailed Communication, entitled *Resilience, Deterrence and Defense: Building strong cybersecurity for the EU*—a joint publication by the Commission and High Representative of the Union for Foreign Affairs and Security Policy.

The Communication and associated documents contain several proposals, some of which—including a new EU cybersecurity certification framework and a permanent mandate for the European Union Agency for Network and Information Security (ENISA)—are included in a new proposed law to be known as the EU "Cybersecurity Act." This will take the form of a regulation and therefore, like the GDPR, apply directly in all Member States, once approved.

The Commission also published and invites feedback on a draft Implementing Regulation on requirements for digital service providers ("DSPs") under the NIS Directive. The consultation is open until **October 11, 2017**.

This alert summarizes key elements of the Cyber Package that we think will be of most interest to our clients.

1. EU Cybersecurity Certification Framework

The Commission is proposing to establish a "European Cybersecurity Certification Framework for ICT products and services" (the "Framework"). The Framework would make use of existing Union and international technical standards and be voluntary, but replace all existing national cybersecurity certification schemes or procedures for ICT products and services.

Why is this new Framework being proposed?

The Commission considers that disparate Member State approaches to cybersecurity certification are impeding the rollout of new products and services and undermining consumer confidence. As Member States currently are free to create their own cyber-related certification initiatives, companies that operate throughout the EU and that seek to certify ICT products may be subject to different procedures and standards. The need for multiple certifications risks the creations of "market fragmentation and interoperability issues," resulting in higher costs for companies.

A certificate issued under one of the Framework schemes would be recognized as valid in all Member States, preventing the need for multiple certificates. The Commission believes that the proposed Framework and European cybersecurity certification schemes will make certification less expensive, more effective, and more commercially attractive, thus helping to spread better cybersecurity practices throughout the EU.

What exactly is the Framework?

The Framework establishes a set of rules to create certification schemes for particular ICT products and services. The Communication mentions as examples the systems that are used in cars, airplanes, power plants, medical devices, as well as Internet-connected consumer devices, among others.

The schemes would define the elements of the certification, including the specific ICT products and services covered, the level of assurances they are intended to ensure (i.e., basic, substantial or high), the detailed specification of the cybersecurity requirements (e.g., by referring to relevant existing Union and/or international standards or technical specifications), and the specific evaluation criteria and methods. Schemes may provide for marks or labels and the conditions for using them.

Who will prepare these schemes?

ENISA will prepare the cybersecurity certification schemes at the request of the European Commission. ENISA will be required to take into consideration input from stakeholders and to coordinate with a new European Cybersecurity Certification Group (consisting of national certification supervisory authorities from all Member States). The Commission will adopt the schemes by means of implementing acts.

Although industry certification schemes are outside of the proposed Cybersecurity Act, it is envisaged that industry may propose to the Commission to consider such schemes to be approved as a European scheme.

What will be the relationship between these European certification schemes and existing standards and national cyber certification schemes?

As set out above, the schemes will not seek to create new technical standards, but instead refer to existing Union and/or international standards or technical specifications.

The Act stipulates that national cybersecurity certification schemes will cease to apply from the date established in the implementing act adopting the new European scheme. In a further attempt to avoid fragmentation, Member States will be required to refrain from introducing new

national certification schemes for ICT products and services that are covered by a European scheme.

Will these schemes be voluntary?

Yes. However, there is a provision, namely that they are voluntary "unless otherwise provided in Union legislation laying down security requirements of ICT products and services." In addition, certification under a scheme may be used to demonstrate the presumption of conformity with requirements of a specific Union act (where the act so provides).

How will organizations apply for certification?

Once a scheme is adopted, manufacturers of relevant ICT products or services would be able to submit an application for certification of their products or services to an accredited conformity assessment body of their choice.

Who will enforce these schemes?

Enforcement is left to the Member States. Each Member State must appoint a national certification supervisory authority that will supervise the compliance of conformity assessment bodies (and certificates issues by these bodies), handle complaints, conduct investigations and audits of certificate holders, and impose penalties for non-compliance.

2. NIS Directive—Incident Reporting and Security Requirements for DSPs

As explained in previous blog posts and alerts, the European Parliament adopted on July 6, 2016 the NIS Directive, otherwise known as the Cybersecurity Directive (*see* our reports here and here). EU Member States have until May 9, 2018 to implement the NIS Directive into national law (recently published UK plans, for example, are summarized here).

Among other things, the NIS Directive imposes security and incident reporting obligations on:

- operators of essential services ("OESs") in the following sectors: energy (electricity, oil, gas); transport (air, rail, road, maritime); banking; financial market infrastructure; health; water supply; and digital infrastructure (IXPs, DNS service providers, and TLD name registries); and
- some digital service providers ("DSPs"), e.g., online marketplaces, online search engines, and cloud computing services.

The security and incident reporting requirements for OESs and DSPs are similar, but DSPs are subject to lighter supervision by competent authorities.

As part of last week's Cyber Package, the Commission has published a separate Communication that sets out best practices and provides guidance on how the NIS Directive should operate in practice. In addition, the Commission has published a draft Implementing Regulation, which specifies further the incident reporting and security obligations for DSPs under the NIS Directive. The Commission invites feedback on this draft up until **October 11, 2017**.

In relation to incident reporting, the draft Implementing Regulation fleshes out parameters to determine whether the impact of an incident is substantial (and thus reportable under Article 16(3) of the Directive). These parameters, which include whether an incident affects the provision of services in two or more Member States, appear to set a relatively low bar for a DSP to have to report an incident to a competent authority. Industry also is likely to have views on the proposed methods to calculate numbers of users—e.g., "the number of affected natural and legal persons with whom a contract for the provision of the service has been conclude" *or,* the number of users "having used the service based in particular on previous traffic data"—in connection with thresholds for downtime (based on user hours and numbers of users affected) that will trigger the reporting requirements.

DSPs also will be interested in a draft provision on security, which sets out "security elements" that DSPs should implement to ensure the security of networks and systems and their physical environment. This provision also lists, among other things, details of technical measures and organizational procedures that should form part of DSPs' incident response capabilities and planning, as well as requirements for policies on auditing and testing systems.

3. Other Aspects of the Cyber Package

As stated at the outset, the Cyber Package contains a plethora of proposals and policy statements, including, for example, in relation to: the uptake of IPv6; challenges with anonymization tools and the darknet in connection with the investigation of criminal offences; public-private partnerships and cooperation mechanisms; Member States' defense capability; and cybersecurity in external relations.

Other elements of the package that are likely to be of most interest to our clients include:

- A stronger mandate for ENISA. The Commission recognizes that ENISA has a key role to play in strengthening EU cyber resilience and response, but also that is it is constrained by its current temporary mandate. The Commission is therefore proposing a permanent mandate for the agency to ensure that it can provide support to Member States, EU institutions and businesses in key areas, including the implementation of the NIS Directive and the proposed cybersecurity certification Framework.
- Potential IoT related regulations. The Communication proposes a joint Commission/industry initiative to define a "duty of care" principle to help reduce the risk of product/software vulnerabilities and promote "security by design." The Communication does not provide details of more specific proposals or a related timeframe, but industry should monitor developments in this area closely.
- Review of product liability rules. The Communication mentions that work is underway to analyze issues concerning liability in relation to new digital technologies. (This is a reference to the ongoing review of the 1985 Product Liability Directive.) Industry and other stakeholders can expect next steps "to be concluded by June 2018," although currently it remains unclear what may be proposed—another area worth monitoring.
- Attacks against information systems. The Commission has published a report on the implementation of the 2013 Directive on Attacks Against Information Systems. This law established minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems, and provided for operational measures to improve cooperation amongst authorities. Although the Commission

commits to continuing to provide support to Member States in their implementation of the Directive, it states that it "currently sees no need to propose amendments to it."

- Proposals to facilitate cross-border access to electronic evidence. The Communication acknowledges that effective investigation and prosecution of cyber-enabled crime is a key deterrent to cyber-attacks, but conceded that "today's procedural framework needs to be better adapted to the internet age." Proposals to facilitate cross-border access to electronic evidence" will be published in "early 2018."
- Fraudulent use of credit cards. The Commission is concerned by the growing threat of fraudulent use of credit card details or other electronic means of payment. It has published a proposed Directive to update existing rules governing online fraud and counterfeiting of non-cash means of payment, following a consultation on the topic earlier this year.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Cybersecurity practice:

Mark Young	+44 20 7067 2101	myoung@cov.com
Kurt Wimmer	+1 202 662 5278	kwimmer@cov.com
Jetty Tielemans	+32 2 549 52 52	htielemans@cov.com
Daniel Cooper	+44 20 7067 2020	dcooper@cov.com
David Fagan	+1 202 662 5291	dfagan@cov.com
James Garland	+1 202 662 5337	jgarland@cov.com

This information is not intended as legal advice. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein.

Covington & Burling LLP, an international law firm, provides corporate, litigation and regulatory expertise to enable clients to achieve their goals. This communication is intended to bring relevant developments to our clients and other interested colleagues. Please send an email to unsubscribe@cov.com if you do not wish to receive future emails or electronic alerts.