Expert Q&A on the EU Cybersecurity Act

Law stated as at 04 Jun 2019 • European Union

An Expert Q&A with Mark Young of Covington & Burling LLP on the EU Cybersecurity Act and its new cybersecurity certification schemes for information and communication technology (ICT) products, services, and processes, especially internet of things (IoT) devices. It also discusses how the Act supports the EU Directive on the Security of Network and Information Systems (Directive 2016/1148/EC) (NIS Directive), the expanded role for the EU Agency for Cybersecurity (ENISA), and what companies need to know about timelines and enforcement.

The EU General Affairs Council formally adopted the Regulation of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communication technology cybersecurity certification (Regulation (EU) 2017/0225) (Cybersecurity Act) on April 9, 2019. This action follows the European Parliament's adoption on March 12. The Cybersecurity Act entered into force on May 7, 2019.

The Cybersecurity Act:

- Reinforces the mandate for ENISA.
- Establishes an EU Cybersecurity Certification Framework (Framework) to:
  - increase the transparency of cybersecurity assurance levels in information and communication technology (ICT) products, services, and processes;
  - improve trust and help end users make informed choices; and
  - lower costs by avoiding conflicting or overlapping national certifications.
- Forms part of the EU's Cyber Package, first announced in September 2017, which seeks to comprehensively strengthen EU cyber resilience (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (JOIN(2017) 450 (Sept. 13, 2017))).

Like the more widely known General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), the Cybersecurity Act is a regulation and once effective applies directly in all EU member states.

Practical Law asked Mark Young of Covington & Burling LLP to discuss the Cybersecurity Act and its new cybersecurity certification scheme for ICT products, services, and processes, especially internet of things (IoT) devices. We also asked Young to discuss how the Act supports the EU Directive on the Security of Network and Information Systems (Directive 2016/1148/EC) (NIS Directive), ENISA's expanded role, and what companies need to know about timelines and enforcement.

Young is a partner in Covington's regulatory and public policy practice with more than 15 years of experience focusing on data privacy, cybersecurity, EU data protection, and intellectual property matters. He counsels clients on protecting business-critical information, complying with national and sector-specific regulation, and preparing for and responding to cyberattacks, data security incidents, and internal threats to their networks and information.

EU Cybersecurity Certification Framework

What are the Framework's key elements?

The Framework creates a mechanism and consistent set of rules for establishing various EU-wide cybersecurity certification schemes. These schemes allow manufacturers and service providers to obtain and share certificates

that verify their cybersecurity controls and status. Under the Framework, certification schemes must:

- Define a clear scope, including the ICT products, services, and processes covered.
- Describe their purpose.
- List specific evaluation standards.
- Provide information on supported assurance levels.
- Indicate whether organizations can self-certify.

(Article 54, Cybersecurity Act.)

The Framework sets three assurance levels aligned with cyber risks. The levels also reflect the rigor and depth of evaluation manufacturers and service providers must undergo to obtain certification. Specifically, the levels and evaluation obligations for ICT products, services, and processes in increasing order are:

- Basic, which:
  - focuses on security controls that minimize known basic cyber risks; and
  - at minimum, requires a technical documentation review or equivalent activity.
- Substantial, which:
  - emphasizes measures to protect against known cyber risks and attackers with limited skills and resources; and
  - at minimum, requires a vulnerability assessment and security controls evaluation and implementation testing or equivalent activities.
- High, which:
  - includes measures to protect against state of the art cyberattacks and significantly skilled, well-resourced attackers; and
  - at minimum, requires a vulnerability assessment, penetration testing, and security controls evaluation and implementation testing or equivalent activities.

(Article 52, Cybersecurity Act.)

What products and technologies are in scope?

The Framework and its cybersecurity certification schemes address ICT products, services, and processes. The regulation broadly defines ICT products as any element or group of elements in a network or information system. ICT services include information transmission, storage, retrieval, or processing services. The less familiar ICT process term refers to activities that organizations engage in to design, develop, deliver, or maintain those products and services. (Article 2, Cybersecurity Act.)

This wide and growing scope includes:

- More traditional ICT, such as computers, network elements, and internet services.
- Information services, such as cloud computing and storage services.
- Emerging technologies, such as:
  - consumer IoT devices, like smart thermostats and appliances; and
  - the connected devices that manufacturers use in cars, airplanes, medical devices, power plants, and other critical infrastructure elements.

Which entities design the schemes and sets the certification standards?

The Cybersecurity Act authorizes the European Commission (Commission) to adopt EU-wide cybersecurity certification schemes that ENISA develops concerning specific groups of ICT products, services, and processes. The regulation emphasizes that these certification schemes should build on existing European or international standards. ENISA is likely to compile and apply current standards, providing additional guidance details, instead

of creating new ones.

The regulation also establishes a Stakeholder Cybersecurity Certification Group of experts charged with advising ENISA and the Commission on cybersecurity certification and related matters.

Is certification voluntary?

The new cybersecurity certification schemes are voluntary. However, the regulation directs the Commission to periodically assess the adopted schemes, their usage, and whether to make specific schemes mandatory. The first review is likely to occur before the end of 2023, with later reviews at least every two years. (Article 56, Cybersecurity Act.)

How are organizations to apply for certificates? Can organizations self-certify their compliance?

The forthcoming schemes are to define specific process details, such as submission and evaluation requirements. National cybersecurity certification authorities in each member state are responsible for implementing and supervising the schemes, but certificates are to be valid EU-wide.

The regulation allows schemes at the basic assurance level to offer conformity self-assessment as an option for ICT products, services, or processes that present a low risk to the public (Article 53, Cybersecurity Act).

What is the relationship between this new Framework and existing national certification schemes?

The Framework's new certification schemes supersede existing national certification schemes to avoid fragmentation. Member states may only create new national schemes for national security purposes.

Companies should view this as a positive development because:

- Mutual recognition among member states for existing national cybersecurity certification schemes has only been partly successful.
- Companies should be able to:
  - avoid certifying to multiple national schemes to participate in national procurement procedures; and
  - submit certification applications to a conformity assessment body of their choice anywhere in the EU.

ENISA's Expanded Role

How is ENISA changing?

The Cybersecurity Act reinforces ENISA's mandate by making it a permanent EU agency, with key roles in implementing the Framework and the NIS Directive, and strengthening cyber resilience across the EU.

What is ENISA's role regarding the Framework?

ENISA is responsible for preparing the Framework's new EU-wide cybersecurity certification schemes. The Cybersecurity Act also tasks ENISA with:

- Maintaining a dedicated website that provides information on and publicizes the schemes, including superseded national cybersecurity certification schemes (Article 50, Cybersecurity Act).
- Disseminating information regarding the cybersecurity levels of ICT products, services. and processes (Recital 51, Cybersecurity Act).
- Issuing warnings to manufacturers or providers of ICT services or processes and requiring them to improve their security measures (Recital 51, Cybersecurity Act).
- Establishing an ENISA Advisory Group to ensure regular dialogue with the private sector, consumer organizations, and other relevant stakeholders (Article 21, Cybersecurity Act).

Interaction with the NIS Directive

What is the NIS Directive?

The NIS Directive, also known as the Cybersecurity Directive:

- Emphasizes cyber resilience for essential services operators and digital service providers.
- Directs EU member states to:
  - transpose its requirements into national law by May 9, 2018;
  - adopt a national strategy on network and information systems security;
  - designate one or more national competent authorities, a single point of contact, and computer security incident response teams (CSIRTs); and
  - develop criteria and identify essential services operators.

- (For current member state implementation details, see EU NIS Directive National Legislation Tracker.)
- Establishes a Cooperation Group to help drive cybersecurity collaboration among the member states.
- Creates a network of the national CSIRTs to support cooperative cyber incident response.

For more information on the NIS Directive, see Practice Note, EU NIS Directive Implementation Activities: Overview.

How do the Framework and the NIS Directive interact?

The Cybersecurity Act and the NIS Directive are both part of the EU's Cyber Package. They focus on complementary activities to drive greater cyber resilience across the EU. The Framework focuses on cybersecurity certification schemes to ensure manufacturers take reasonable cybersecurity measures upfront in their ICT products, services, and processes. The NIS Directive emphasizes cyber incident preparedness and cooperative response planning and management.

Timelines and Enforcement

What is the Framework's implementation timeline and what happens next?

The regulation calls on the Commission to prepare a "Union rolling work programme for European cybersecurity certification" within one year of the regulation's effective date (Article 47, Cybersecurity Act). The work plan should include a list of ICT product, service, and process categories targeted for the certification schemes, including timelines and priorities.

Which entities enforce the certification schemes and are maximum penalties set?

National cybersecurity certification authorities in the member states are responsible for implementing and supervising the schemes.

Certification schemes that industry or other private organizations operate are outside of the regulation's scope. However, these regimes can seek approval as formal European cybersecurity certification schemes.

EU member states intend to establish penalties for infringing the cybersecurity certification schemes. The regulation requires that penalties are:

- Effective.
- Proportionate.
- Dissuasive.

(Article 65, Cybersecurity Act.)

What should organizations do now?

Manufacturers and service providers should:

- Prepare for certification by reviewing their current ICT products, services, and processes against widely accepted international standards and security by design principles, such as the ISO 27xxx family of standards and current ENISA best practice guidance.
- Monitor the Commission's work program and progress for new certification scheme implementation dates.

Buyers, including businesses and consumers of ICT products, services, and processes, should begin asking sellers about their cybersecurity certification plans and the information security standards and principles that they follow.

