POLSINELLI

Publications

February 28, 2025 • Updates

Examining Cybersecurity Critical Infrastructure Regulations in the U.S. and EU

Business entities within the critical infrastructure sector provide essential products and services for the public, and disruptions to these entities' operations arising from a cyberattack can threaten national security and public safety. This reality was illuminated after the 2021 cyberattack on Colonial Pipeline. Last year, Tom Fanning, the chair of the Cybersecurity and Infrastructure Security Agency's (CISA) Cybersecurity Advisory Committee, provided a retrospective on this watershed moment in American history, reflecting:

"On May 7, 2021, a ransomware attack on Colonial Pipeline captured headlines around the world with pictures of snaking lines of cars at gas stations across the eastern seaboard and panicked Americans filling bags with fuel, fearful of not being able to get to work or get their kids to school. This was the moment when the vulnerability of our highly connected society became a nationwide reality and a kitchen table issue."

One need only peruse CISA's list of the types of companies that fall within the critical infrastructure sector – hospitals, food and agricultural businesses and banks – to appreciate what large-scale cyberattacks against those types of organizations could similarly mean for the American public. This is especially true in light of warnings from the U.S. government about potential cyberattacks against critical infrastructure from nation state actors out of China and Russia.

Securing critical infrastructure is not a singularly American concern. As is typical when it comes to data security and privacy regulation, the European Union has led the way globally in terms of prophylactic regulations. While the U.S. government has outwardly expressed alarm and focus on this topic, it has not taken the same hands-on approach as its European counterparts. The U.S. government has largely left the implementation of technical controls within critical infrastructure to industry group development and private participation.

The policy challenges of regulating millions of primarily private-sector companies in the U.S. have enabled an amalgamation of overlapping and complex reporting requirements

Related People

- Sarah S. Glover
- Gregory J. Leighton
- Romaine C. Marshall
- Mary Ann H. Quinn

Related Capabilities

- International Privacy
- Privacy & Cybersecurity

and a lack of prescriptive security controls to date.

Examining and contrasting the controlling critical infrastructure frameworks in the EU and U.S. might shed some light on where the U.S. could be headed if it decides to ramp up regulations in this space. And, for those U.S. companies that are operating in the EU, it is important to understand the developing critical infrastructure regulatory landscape that they may already be subject to abroad.

European Critical Infrastructure Security Framework

In 2006, the European Union issued the Communication from the Commission on a European Programme for Critical Infrastructure Protection (EPCIP). At this time, policymakers and lawmakers were primarily focused on protecting critical infrastructure from terrorist attacks, so the EPCIP did not mention cybersecurity or set out any specific security controls. However, the EPCIP did set out a protection framework based on an "all-hazards" approach, which included:

- A procedure for identifying and designating entities providing critical infrastructure;
- An information-sharing process and plan, including a warning network and use of expert groups;
- Support for member states;
- Contingency planning.

The EPCIP framework became the backbone of the Network and Information Systems Directive (NIS1), signed in 2016. NIS1 was the EU's first piece of EU-wide legislation on cybersecurity, and it provided for legal measures to boost the overall level of cybersecurity in the EU, but with a focus on critical infrastructure. NIS1 established the NIS Cooperation Group, as well as a network of Computer Security Incident Response Teams to facilitate the exchange of information and the provision of support during actual incidents, respectively.

While NIS1 was being transposed to the laws of the EU's member states, the threat landscape continued to evolve into the cyber domain, and by 2019, EU officials noted a continuing lack of cyber resilience of businesses across critical infrastructure sectors. These concerns motivated EU lawmakers to further define and update the scope of the law to create a piece of legislation that had staying power to meet current risks and future challenges in a rapidly changing environment.

NIS2 is the recent product of this effort and is currently a hot topic across industries for organizations operating in the EU. Signed in 2022 and going into effect in January of 2025, NIS2 is the most recent and most widely applicable critical infrastructure regulation in the EU. It is less voluntary than NIS1, covers more industries and prescribes specific cybersecurity measures for critical infrastructure entities. NIS2 requires the EU member states to implement NIS2's requirements for both public and private entities. Specifically, NIS2 requires that member states ensure that covered entities take appropriate technical, operational and organizational measures that include:

- Policies on risk analysis and information system security;
- Incident handling;
- Business continuity, such as backup management and disaster recovery, and crisis management;
- Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
- Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

- Policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
- Basic cyber hygiene practices and cybersecurity training;
- Policies and procedures regarding the use of cryptography and, where appropriate, encryption;
- Human resources security, access control policies and asset management;
- The use of multifactor authentication or continuous authentication solutions; secured voice, video and text communications; and secured emergency communication systems within the entity, where appropriate.

While it does contemplate security measures for suppliers, NIS2 does not directly regulate them or define the scope of the affected supply chain. Entities that are preparing for NIS2 compliance may begin to flow down certain security requirements to their partners, such as the requirement to conduct risk assessments, establish incident reporting and vet security controls. So third parties and suppliers can expect to see NIS2 initiatives trickle down into their contracts with covered entities.

Other critical infrastructure security frameworks exist within the EU, such as the Digital Operations Resilience Act (DORA) proposal for the financial sector and the European Electronic Communications Code (EECC). These frameworks are meant to function together with NIS2 in the interest of maintaining a strong relationship and exchange of information between the sectors covered by NIS2. Where DORA, for example, provides for more stringent security requirements for financial companies, NIS2 is meant to establish a security baseline across all sectors.

U.S. Critical Infrastructure Security Framework

After 9/11, the Department of Homeland Security (DHS) was positioned to bring the core homeland security initiatives under more-unified leadership, but critical infrastructure regulation remains highly distributed throughout the federal government even today.

One of the foundational critical infrastructure policy documents marking the shift away from counter-terrorism security was the 2013 Presidential Policy Directive 21 (PPD-21), which placed less focus on the dangers of terrorism and more focus on an all-hazards approach. PPD-21 contains the most widely accepted definition of “critical infrastructure” as the systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

PPD-21 also named 16 critical infrastructure sectors, and approximately 13 million business entities make up these sixteen sectors as of April 2024.

As depicted below, DHS is one of several Sector Risk Management Agencies (SRMAs) responsible for critical infrastructure security regulation.

16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

In addition to these SRMAs, other agencies have issued industry-specific regulations regarding cybersecurity incident reporting for critical infrastructure entities, including the Federal Communications Commission, Nuclear Regulatory Commission and Securities and Exchange Commission.

In 2018, CISA was established as an operational component of DHS charged with "mobilizing a collective defense to understand and manage risk to our critical infrastructure and associated National Critical Functions" as they relate to cyber and physical threats. CISA is at the center of a new rulemaking effort to establish the implementing framework for the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) (6 U.S.C. §§ 681-681g), enacted in March of 2022. CISA released a notice of proposed rulemaking on March 27, 2024, that requires in part that critical infrastructure companies report cybersecurity incidents within 72 hours. This reporting requirement is not a replacement for all of the other sector-specific incident reporting obligations described above. The final rule is expected sometime in 2025, with reporting requirements taking effect in 2026. While CISA seems to be poised to eventually be the home base for critical infrastructure security regulation, CIRCIA does not contain, in the statute or in the proposed rulemaking, a list of specific controls and requirements to elevate the security baseline for critical infrastructure companies in the U.S.

Additionally, CISA just released the proposed National Cyber Incident Response Plan (NCIRP), on December 16, 2024, for public review and comment. The NCIRP outlines a proposed framework for how federal, private sector, state and international partners can cooperate to respond to incidents. It also outlines the roles and responsibilities of the various agencies that may be involved in a response to an incident impacting critical infrastructure. Finally, the NCIRP contains a proposed classification and severity-level matrix, informing stakeholders how CISA intends to distinguish the lower-level "Baseline" incidents from higher-level "Severe" or "Emergency" incidents. The proposed NCIRP provides helpful insight into CISA's incident response and coordination priorities. Critical infrastructure entities should use the proposed NCIRP, and the forthcoming final version, to guide the ongoing review (or development) of their incident response plans and programs. Incident response planning is poised to remain a top regulatory concern for critical infrastructure in the coming months and years.

Check out our previous article for more information on CIRCIA.

What Is Next for Critical Infrastructure Entities in the U.S.?

The focus of U.S. critical infrastructure cybersecurity regulation to date has been on information sharing and gathering, while the EU has already begun to regulate prophylactic security controls. EU policymakers will debate the distribution of risk, the burden of compliance and the improved readiness as these laws continue to take effect over the next year. Many suspect that U.S. lawmakers will wait to observe NIS2's impact on European critical infrastructure entities before making moves to implement similar broadly applicable legal frameworks.

For now, any U.S. companies within critical infrastructure would be wise to focus on incident response planning and incident response readiness – including the logging and monitoring (of people, processes and technology) necessary to enable quick detection of incidents – as this will likely be the first security domain with any real regulatory momentum in the states. If and when we do see more prescriptive security requirements in the U.S., they will likely simply codify well-established industry best practices, like those reflected in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (Version 2.0) and CIS Critical Security Controls (Version 8.1). Any companies that have not already done so should go ahead and focus on building out and assessing their security programs to align with these frameworks.