Cybersecurity Law Report cslawreport.com

Oct. 12, 2022

Incident Response

A New Era of Cyber Incident Reporting and Cybersecurity Regulation: Key Provisions

By
Gregory Gonzalez, Evelyn Remaley, Brian Murray, Clete Johnson, Savannah Schaefer, Morgan Schick and Karina Bohorquez,
Wilkinson Barker Knauer LLP

To the surprise of many in Washington, it was a kinetic event – not a cyberattack – that launched a new era of cybersecurity policy in the United States. On March 15, 2022, just weeks after Russia's invasion of Ukraine, the United States Congress enacted the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), giving the Cybersecurity and Infrastructure Security Agency (CISA), within the Department of Homeland Security (DHS), its first, and perhaps not last, rulemaking authority.

This first article in a two-part series examines important provisions of CIRCIA that CISA, with industry input, will shape through this rulemaking process. Part two identifies areas that should warrant particular concern and attention from companies in the financial services, communications and energy sectors. As the most significant critical infrastructure sectors, developments in each will influence the others and collectively drive the pace and nature of cybersecurity regulation more generally; as such, none of them can be fully understood in a vacuum. Part two also addresses what all of this means for the future of cybersecurity regulation in the United States.

See "Lessons From CISA for In-House Counsel on Mitigating and Managing MSP Breach Threats" (Jun. 29, 2022).

Impetus for a Change in the Paradigm

Cyber events disrupting U.S. critical infrastructure, like the denial-of-service attacks on financial institutions in 2011 and an electricity provider in 2019, had occurred with some consistency over the previous decade. But, in 2021, the stakes were raised when ransomware attacks against Colonial Pipeline and JBS Foods occurred in quick succession, disrupting the fuel supply to the East Coast and temporarily halting food production by the largest meat supplier in the country. The U.S. government itself has been the victim of several major breaches, including the Office of Personnel

Management, in 2015, and the software supply chain attack on SolarWinds, which was discovered in 2020 to have compromised data across numerous federal agencies, as well as private corporations. Still, the U.S. government did not act to compel the private sector to report cyber incidents.

For decades, the U.S. government's focus has been on building and maintaining public-private partnerships to foster voluntary exchanges of information, both for cyber-defense and law-enforcement purposes. That posture was enshrined in the Cybersecurity Information Sharing of Act of 2015 (CISA 2015), which remains in effect, even with the passage of CIRCIA. Where policymakers have wanted to build capacity or drive adoption of cybersecurity capabilities and practices, it has done so through federal procurement – rules the government places on itself – to simultaneously enhance the government's cybersecurity posture and influence the broader market through federal purchasing power. Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," signed by the President in May 2021, initiated sweeping requirements across federal agencies to do just that.

CIRCIA marks a change in the paradigm. When the final rules for CIRCIA are implemented, certain companies within the 16 critical infrastructure sectors, including three of the most significant sectors – financial services, energy, and communications – will be required to report covered cyber incidents to CISA within 72 hours and ransom payments within 24 hours. Fortunately, the current messaging from CISA indicates that, although there are new statutory requirements and basic enforcement powers associated with CIRCIA, the agency wants to maintain its position as the facilitator of the collaborative, public-private partnership model that enables it to perform its defensive cyber functions alongside critical infrastructure owners and operators (which are overwhelmingly private sector entities). This desire to work collaboratively with industry extends to the CISA rulemaking process that is now underway. That said, there are proposals already circulating in Congress, subject to inclusion in the upcoming 2023 National Defense Authorization Act, that would establish cross-sector and sector-specific cybersecurity "performance goals" for a subset of critical infrastructure entities deemed "systemically important." This would potentially move CISA into a much more authoritative regulatory position, even if it is not actively seeking that role.

CISA must by statute promulgate final rules for CIRCIA by September 2025, although it is likely facing significant intragovernmental pressure to implement the statute much sooner. One step in that process is receiving feedback from the public and, on September 21, 2022, CISA began the first of 11 listening sessions to be held at various locations around the country, including one happening on October 12, 2022, in New York, giving the financial sector and other critical infrastructure companies an opportunity to inform the rulemaking process. These listening sessions are intended to complement the pending Request for Information, published in the Federal Register in September 2022, which will close on November 14, 2022. CISA also plans to hold sector-specific listening sessions before issuing a Notice of Proposed Rulemaking, which will be followed by formal written comments from companies potentially impacted by the future rules.

See "CISA and DHS Counsel Explain Cybersecurity Executive Order's Key Provisions" (May 26, 2021).

CIRCIA Scoping Definitions

"Covered Entities"

CIRCIA does not specify what entities should be covered, other than to require that they be part of a critical infrastructure sector, as defined in Presidential Policy Directive 21, which identifies the current list of 16 critical infrastructure sectors used for preparedness planning today. Under CIRCIA, the final rule must include: a clear description of "covered entities" based on: (1) the consequences that disruption to or compromise of such an entity could cause to national security, economic security or public health and safety, (2) the likelihood that such an entity may be targeted by a malicious cyber actor, including a foreign country, and (3) the extent to which damage, disruption or unauthorized access to such an entity will likely enable the disruption of the reliable operation of critical infrastructure. With this qualifying language, Congress made clear its belief that not all entities that are technically part of a particular critical infrastructure sector should necessarily be included within the scope of CIRCIA's cyber incident reporting requirements. CISA will need to balance its interest in seeing a broader swath of the threat surface with the ability to effectively aggregate and analyze relevant data to build a shared understanding of threats and trends.

"Covered Cyber Incidents" and the "Reasonable Belief" Standard

CIRCIA provides few details about the types of cyber incidents that will be covered, other than that they must be "substantial." The final rule must include a clear description of the types of cyber incidents that are "covered," which will, at minimum, require the occurrence of: (1) a cyber incident that leads to substantial loss of confidentiality, integrity or availability of an information system or network, or a serious impact on safety and resiliency of operational systems and processes; (2) a disruption of business or industrial operations, including a denial-of-service attack, ransomware attack, or exploitation of a zero-day vulnerability, against an information system or network or an operational technology system or process; or (3) unauthorized access or disruption of business or industrial operations due to a loss of service facilitated through, or caused by, a compromise of a cloud service provider, a managed service provider, a third-party data hosting provider, or by a supply chain compromise. In establishing the rule, DHS is required to consider: (1) the sophistication or novelty of the tactics used to perpetrate such a cyber incident, (2) the type, volume and sensitivity of the data at issue, (3) the number of individuals directly affected or potentially affected, and (4) the potential impacts on industrial control systems.

During the rulemaking process, CISA likely will provide guidance to companies as to when a "reasonable belief" exists that triggers the reporting of a covered cyber incident. CISA also likely will require covered entities to document a negative reasonable belief determination. While there are conceivable disagreements between CISA and covered entities on when such reasonable belief exists, in practice, CISA probably will rely on the good faith of companies to report incidents, with only the most egregious circumstances warranting the invocation of CISA's subpoena authority and potential civil subpoena enforcement litigation (discussed below). However, CISA should seek to provide as much clarity as possible in defining the boundaries so that companies are not spending valuable incident response resources and attention determining whether the incident is substantial and to prevent CISA from being bombarded with immaterial reports.

See "How to Prepare for the Cybersecurity Incident Reporting for Critical Infrastructure Act" (Aug. 3, 2022).

Protections Afforded to Reporting Companies

Civil Litigation Arising from Reporting

CIRCIA states that no cause of action shall lie, in any court, by any person or entity, for the submission of a report, other than an authorized civil action to enforce a CISA administrative subpoena. However, this protection only applies if the litigation is "solely based" on the submission of a covered cyber incident report or ransom payment report to CISA (information voluntarily provided to CISA through this process is similarly protected). If the report to CISA is confidential and secure, and the information provided to stakeholders and the public is anonymized, it is unclear how a civil action could be filed that is solely based on the submission of a report. This means that, without additional rulemaking, the civil immunity provision may be of little consolation to reporting companies.

Regulatory Actions Generated From Reporting

Unlike CISA 2015, which established a categorical prohibition on the use of information provided by the private sector, CIRCIA only provides limited immunity to covered entities. According to CIRCIA, the information reported by a covered entity "shall not" be used by federal, state, local or Tribal governments for regulation, including an enforcement action. However, the statute states that this prohibition applies only to information obtained "solely" through the reporting submitted to CISA. That means that if the information reported were to also come from another source before, contemporaneously or after the information is provided to CISA, it can be used for an enforcement action against the covered entity, even if the information was also submitted in an incident report. This may very well lead to extensive litigation about the sourcing of information obtained by a regulator if used in an enforcement action against an entity that reported similar information to CISA.

The information contained in the reports to CISA can also be used by a regulatory agency if that agency affirmatively allows entities to submit the CIRCIA report to meet regulatory reporting obligations. This provision should encourage regulatory agencies to accept the form submitted to CISA to meet their own regulatory requirements, thereby reducing the regulatory burden on covered entities as they seek to respond and recover from a covered cyber incident. However, given the likelihood that regulatory agencies will obtain information about covered cyber incidents through means other than the CISA reporting (*i.e.*, media reporting), some agencies may choose to maintain their own, potentially more burdensome, reporting requirements, circumventing the protections Congress intended to afford to covered entities in CIRCIA. If that becomes a practice of regulators in critical infrastructure sectors, such as the SEC, the Federal Communications Commission (FCC), or the Federal Energy Regulatory Committee (FERC) for energy companies, covered entities would

need to consider whether to file a uniform report and focus on incident remediation, as opposed to providing potentially disparate information, to multiple regulators, while an incident is ongoing.

Protection of Legal Privileges and Business Confidential Information

Importantly, under CIRCIA, a report does not constitute a waiver of "any applicable privilege or protection provided by law." This preserves the ability of a covered entity to invoke attorney-client privilege and work-product protections if regulatory or civil litigation ensues after a report is made. It also allows companies to protect trade secrets. Further, information reported to CISA can be designated by the covered entity as commercial, financial and/or proprietary, although the statute does not describe the effect of each designation, particularly since the reports themselves will not be shared with the public and are exempt from federal, state, local and tribal freedom of information laws.

According to the statute, the report itself and any communications, documents, materials or other records created for the "sole purpose" of preparing, drafting, or submitting such report are not discoverable and not admissible in any trial, hearing or other proceeding in or before any court, regulatory body, or other authority of the United States, a state or a political subdivision thereof. However, this appears to contradict the provision that allows for regulatory enforcement based on information obtained solely through a report when the report is also accepted by the regulatory agency to meet agency-specific requirements. Given the apparent intent to afford substantial protections to reporting companies, CISA likely will give these provisions significant attention during the rulemaking process and will need to ensure that Congressional intent is upheld.

See "Steps to Protect Privilege for Data Breach Forensic Reports" (Jan. 27, 2021).

Enforcement: No Financial Penalties for Non-Compliance

CIRCIA does not provide statutory authorization for financial penalties to be assessed against companies for non-compliance. CISA will have the authority to carry out its regulatory role using administrative subpoenas which can be issued if a voluntary request for information goes unanswered or if the response to CISA is deemed to be inadequate. Enforcement of an administrative subpoena issued by the CISA Director can be referred to the Department of Justice, which can bring a civil action and seek a contempt of court finding and remedies. Any information produced in response to an administrative subpoena can be provided by the CISA Director to a regulatory or law enforcement agency, negating any of the protections for reporting companies established by statute and incorporated into the final rules.

See "Implementing NSA-CISA-FBI Advisory Mitigation Tactics for Vulnerabilities Exploited by Russia" (Apr. 28, 2021).

The Newly Established Cyber Incident Reporting Council

CIRCIA established a Cyber Incident Reporting Council (CIRC), which requires the Secretary of Homeland Security, along with the Director of the Office of Management and Budget, the Attorney General, the National Cyber Director, sector risk management agencies (Treasury Department for the financial services sector, DHS for the communications sector, and the Department of Energy for the energy sector), and other appropriate federal agencies, including the SEC and the FTC, to "coordinate, deconflict, and harmonize federal incident reporting requirements, including those issued through regulations." This requirement does not provide additional regulatory authority to any federal department or agency; neither does it constrain other departments or agencies from imposing additional reporting requirements that go beyond the scope of a "covered cyber incident" report. The CIRC will also assist CISA in establishing supplemental reporting requirements, giving due consideration to existing regulatory reporting requirements.

While the CIRC does not allow DHS to set cyber incident reporting requirements across the federal government, it manifests Congressional intent that some deference be given to DHS, and the other statutorily identified partners, as the deconfliction process moves forward. The CIRC had its first meeting in July 2022, which was chaired by the DHS Secretary. According to a media release, following the meeting, the Secretary expects that the CIRC will "meaningfully improve cybersecurity, reduce burdens on industry by advancing common standards for incident reporting, and inform a report from the Secretary," due to Congress within 180 days of the first CIRC meeting (on January 18, 2023), which will present recommendations for how the federal government can achieve harmonization of reporting requirements.

See "Task Force Leader Addresses Proposed Mandatory Reporting of Ransomware Payments" (May 26, 2021).

Gregory Gonzalez is a partner at Wilkinson Barker Knauer (WBK), LLP, in Washington D.C. He is a former career Department of Justice national security prosecutor, intelligence lawyer and counsel to National Security Division leadership. Gonzalez was designated as a National Security Cyber Specialist for over seven years and received advanced cyber training as an National Security Division Cyber Fellow. In that role, he successfully investigated and prosecuted a first-of-its-kind national security-cyber case. In his final position with DOJ, he served as the Department's first Liaison to U.S. Cyber Command. At WBK, Gonzalez counsels clients on a wide array of national security, cybersecurity, and data privacy matters.

Evelyn Remaley is a partner at WBK. Before joining the firm, she was Acting Assistant Secretary of Commerce for Communications and Information, and Acting Administrator of the National Telecommunications and Information Administration, an Executive Branch agency, part of the Department of Commerce, that is principally responsible for advising the President on telecommunications and information policy issues. In that role, Remaley was also responsible for leading the Department's cybersecurity policy efforts. Prior to her federal service, she led a cybersecurity and internet policy team at Booz Allen Hamilton, where she oversaw efforts supporting a wide range of cyber policy and governance projects for the Departments of Defense and Homeland Security.

Brian Murray is a partner at WBK. He has been a practitioner of communication law in private practice for two decades. Murray's substantive experience encompasses cybersecurity, the regulatory treatment of IP-based services and the implications of foreign investments in the U.S. He is also well-versed in many traditional telecommunications and media regulatory issues.

Clete Johnson is a partner at WBK and a U.S. Army veteran. Prior to joining WBK, he served as a senior cybersecurity counsel in a variety of roles in the national security and intelligence communities, including as Professional Staff for the Senate Select Committee on Intelligence, Chief Counsel for Cybersecurity at the Federal Communications Commission, and Senior Adviser for Cybersecurity and Technology to the Secretary of Commerce, serving as the Commerce Department's primary staff representative for National Security Council deliberations on cybersecurity matters.

Savannah Schaefer is an associate at WBK. Prior to joining WBK, she led cybersecurity policy development for two technology and telecommunications-focused trade associations. She served in leadership roles on the Information Technology Sector Coordinating Council and the Department of Homeland Security's ICT Supply Chain Risk Management Task Force, and as a member of the Communications Sector Coordinating Council. Additionally, Schaefer served as a fellow at the Federal Communications Commission.

Morgan Schick is an associate at WBK. She advises clients on a wide array of communications issues, including network security, public safety and wireless resiliency.

Karina Bohorquez is an associate at WBK. Prior to joining WBK, she interned with Freedom Technologies Inc., NTIA's Office of Policy Analysis and Development, T-Mobile government affairs, and USTelecom's policy and advocacy team.