October 16, 2023

Skadden

Privacy & Cybersecurity Update

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
212.735.3000

Federal Report Proposes Harmonization of Divergent Cyber Incident Reporting Regimes

On September 20, 2023, the U.S. Department of Homeland Security released a report outlining the varied and sometimes conflicting reporting requirements that private entities face when they are victims of a cyber incident. The document (Report), drafted with input from the leaders of 33 departments and agencies, offers detailed proposals to harmonize definitions and reporting procedures, and reduce or eliminate duplicative and inconsistent requirements by coordinating the efforts of different branches of the federal government. It also recommends legislative changes where streamlining cannot be achieved without changes to existing law.

The report was required by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), which President Biden signed into law March 2022. CIRCIA created the inter-agency Cyber Incident Reporting Council (CIRC), which drafted the Report.

The Report's proposals are discussed in detail below, but key takeaways for private sector entities with reporting requirements include:

- **Analysis of duplicative reporting requirements.** In all, the Report identifies 45 unique federal reporting requirements established by statute or regulation and administered by 22 federal agencies. Moreover, the Report highlights seven proposed new or amended reporting requirements that are currently under consideration.
- **Proposal for standardized definitions.** The Report recommends a model definition to standardize the meaning of "cyber incident." Incidents that are under investigation would still be reportable, but data breaches where compromised data was adequately encrypted would be excluded from reporting requirements.
- **Recommended cyber incident reporting requirements.** To harmonize conflicting requirements, the Report proposes a government-wide 72-hour reporting requirement for *most* cyber incidents, but recognizes that national security and public health breaches may require a shorter timeline. CIRC recommends that the "timer" start when a company "reasonably believes that a reportable cyber incident has occurred."

At present, there is no legislation pending to address these issues. Some agencies may implement certain recommendations through rulemaking, and the president could issue an executive order to streamline reporting requirements within the bounds of existing law.

Federal Report Proposes Harmonization of Divergent Cyber Incident Reporting Regimes

However, CIRC recognizes that enduring, whole-of-government change ultimately requires congressional action, and the Report makes specific legislative recommendations.[1]

Findings on Duplicative Incident Reporting

The Report first reviews the patchwork of federal reporting requirements that companies confronting a cyber incident must navigate. For instance, the Report outlines duplication in sector-specific, cross-sector and voluntary federal reporting requirements, in addition to disparate local, state and foreign reporting obligations. Duplicative sector-specific reporting requirements discussed in the report include the following sectors:

- **Transportation sector.** If a single incident impacts varied modes of transportation, entities in the transportation sector may need to navigate multiple reporting obligations. The U.S. Coast Guard requires that the owners and operators of vessels, waterfront facilities and outer continental shelf facilities submit reports of certain security breaches, including cyber incidents. The Transportation Security Administration maintains eight separate reporting requirements, covering aircraft and airport operators, cargo screening facilities, passenger and freight rail carriers, rail transit systems, natural gas pipelines and liquid natural gas facilities. Natural gas facilities may have to notify the Department of Energy (DOE), and covered defense contractors may have obligations to the Defense Department under the Defense Federal Acquisition Regulation Supplement.
- **Public health sector.** A company operating in the public health sector might need to report cyber incidents to the Department of Health and Human Services (HHS), the Federal Trade Commission (FTC) and the Food and Drug Administration (FDA). For instance, the Health Insurance Portability and Accountability Act (HIPAA) Breach Notification Rule requires certain health care providers and plans to report data breaches to HHS. If an incident also affects a medical device, a report to the FDA may be necessary as well.
- **Financial services sector.** The Report notes that eight different federal agencies have requirements for reporting cyber incidents in the financial sector. For instance, in addition to obligations to provide suspicious activity reports to the Treasury Department's Financial Crimes Enforcement Network, some entities may need to report cyber incidents to the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Federal Reserve Board or the Commodity Futures Trading Commission.
- **Communications sector.** Communications providers must report any outage reaching a certain threshold, including outages caused by a cyber incident, to the Federal Communications Commission (FCC). But the FCC also requires telecommunications carriers and interconnected VoIP service providers to inform law enforcement agencies when a breach of their customers' proprietary network information (CPNI) occurs, so an outage that involves the breach of CPNI would require two separate reports. Furthermore, Executive Order 13913 (Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector) requires FCC licensees and authorization holders that operate critical telecommunications infrastructure to notify the Department of Justice (DOJ) within 48 hours.

Additionally, many entities covered by single-sector regimes might have also have additional reporting obligations under rules like the Securities and Exchange Commission's (SEC's) public company reporting requirements.

The CIRC recognizes that, while some agencies establish reporting requirements to address breaches involving sensitive personal or commercial data, others are motivated by national security, public health, or consumer and investor protection. However, CIRC acknowledges the burden of such competing requirements on the private sector based on comments it received from non-governmental stakeholders during its review.

Challenges to Harmonization

The Report identifies five critical areas requiring harmonization:

- **Inconsistent definitions.** Key definitions vary widely. For instance, the threshold for a reportable incident can range from "serious impact" to "substantial loss" to a "disruption." In some instances, the mere possibility of an adverse effect suffices to trigger a reportable incident.[2]
- **Timelines.** The deadlines to report a cyber incident also vary across agencies. CIRC found that the time span for consumer protection and privacy reports ranges from a week to two months after the discovery of a data breach. However, agencies focused on national security or economic security typically require reports in a matter of hours or days.[3]
- **Triggers.** Different regimes "start the clock" for reporting requirements at different points. Some begin when an incident is discovered, while others employ a reasonableness standard. A

[1] Even if the U.S. Congress passed legislation in line with the Report's recommendations, companies would still be required to comply with varied laws at the state and local level. However, it is possible that successful efforts to harmonize definitions, forms and requirements at the federal level could catalyze similar harmonization at the state and local level.

[2] Department of Defense, Defense Federal Acquisition Regulation Supplement, 252.204-7012.

[3] Consumer protection and privacy frameworks include entities covered by HIPAA, the FTC and FCC. National security and economic security entities include the DOJ and SEC.

third category of rules employ a more subjective standard, only requiring reports once a company "makes the determination that" an incident is reportable.[4]

- **Report content.** The content required in reports differs under different regimes. While some only require a basic narrative description of the incident, others require a much more technical readout on threat information and operational consequences.[5]
- **Reporting mechanisms.** Agencies employ quite different mechanisms for reporting incidents. Some provide specific formatting guidelines and maintain online web portals or secure file transmission systems. Others request narrative reports via mail, email, fax or phone with no formatting guidance. In some cases, agencies will accept or recognize forms promulgated by other agencies, but the vast majority do not.

Model Definitions and Recommendations for Regulatory Change

CIRC proposes eight recommendations to facilitate a harmonized cyber incident reporting system:

- **Standardized definition of a reportable cyber incident.** The Report provides a model definition for reportable cyber incidents and recommends that the federal government adopt such a standardized definition wherever possible. In order to promote timely reporting, the model definition clarifies that incidents under investigation are still reportable. However, the Report recommends that agencies consider excluding the reporting of data breaches when compromised data was adequately encrypted or dissociated and cannot be exploited.
- **Model cyber incident reporting timelines and triggers.** CIRC acknowledged that different timelines may be appropriate for different agencies based on their mission. The Report therefore recommends a basic 72-hour reporting requirement, but with carve-outs for "the delivery of national critical functions … public health or safety" that may require shorter timelines, and certain data breaches where a longer timeline may be appropriate. For all cases, however, the Report recommends an objective trigger provision, proposing that the clock starts when a company "reasonably believes that a reportable cyber incident has occurred."
- **Delayed public notifications.** The Report recommends that agencies adopt an option for delayed public disclosure where an announcement might impact law enforcement or national security activities.
- **Model reporting form.** The Report proposes that agencies adopt a standardized reporting format with common data elements. Those agencies with unique mission needs could add additional modules as required. Similarly, those agencies with statutory limitations on their collection capabilities could craft a customized form covering only those elements that are permitted.
- **Streamlined receipt and sharing of cyber incident reporting.** The Report recommends a federal study to examine the sharing of cyber incident reports across the agencies.
- **Permit updates and supplemental reports.** Recognizing that victims possess limited information during the initial phases of a response, the Report suggests that agencies should permit companies to supplement their reports as new information and analysis becomes available. To expedite incident reporting, agencies should clarify what information is essential for the initial report and what information companies can provide in an update.
- **Establish common lexicon for cyber incident reporting.** In order to streamline initial reporting and ensure transparency, agencies should harmonize terminology. The Report includes a list of common terms and proposed definitions in an appendix.
- **Improved processes for engaging with reporting entities.** CIRC's outreach identified private sector concerns that uncoordinated federal outreach wastes limited time and resources during incident response. Therefore, the Report urges the Cybersecurity and Infrastructure Security Agency, federal law enforcement and federal regulators to coordinate internally before reaching out to a reporting party.

Legislative Recommendations

As required under the CIRCIA, the Report also proposes three specific legislative actions:

- The Report notes that statutory requirements preclude some agencies from adopting new provisions, such as the proposed definition for a reportable cyber incident or harmonized timelines and triggers. CIRC therefore recommends that Congress consider legislation authorizing agencies "to align their regulatory requirements to CIRC recommendations notwithstanding other provisions of law."
- Agencies participating in the drafting of the report expressed concern that a harmonized reporting form could run afoul of statutory limitations on what information they can legally collect. The Report therefore recommends that Congress authorize agencies to "collect and share with each other 'common data elements' [that] will assist in harmonizing the information" they may collect in cyber incident reports. In the Report, CIRC acknowledges that any expansion of collection authority must be carefully balanced with privacy, civil rights and civil liberties concerns.

[4] CIRCIA has a 72-hour reporting timeline. Cyber incidents in the Nuclear Reactors, Materials, and Waste Sector must be reported in one to eight hours. The DOE has a one-hour timeline after the determination of a reportable cyber security incident. Finally, SEC requires immediate reporting for certain regulated entities.

[5] Generally, reporting requirements in the context of national security, economic security or public safety regimes focus on technical threat information and operational consequences of the incident. Privacy and customer protection regimes focus more on the nature of information accessed or stolen and the risk of harm to individuals affected.

Federal Report Proposes Harmonization of Divergent Cyber Incident Reporting Regimes

- CIRC also recommends in the Report that Congress exempt cyber incident reported information from disclosure under the Freedom of Information Act. During its outreach, CIRC learned that companies fear that information they report will be disclosed, as reports to different agencies receive different protections.

Concerns and Recommendations of Private Stakeholders During Outreach

In addition to CIRC's own proposals, the Report summarizes the concerns voiced by industry stakeholders during CIRC's outreach process. Their suggestions included:

- The federal harmonization of incident reporting should take into account state, local and foreign requirements.
- The federal government should make sure entities are not liable for good-faith efforts to comply with the reporting requirements.
- The federal government should ensure that sensitive cyber incident information reported by the private sector is protected from disclosure, including but not limited to protections of the Freedom of Information Act and applicable privileges.
- The federal government should provide anonymized or aggregated information from incident reports to reporting entities and work closely with information sharing and analysis centers (ISACs) and information sharing and analysis organizations (ISAOs) that serve as clearing houses for information about cyber incidents.
- The federal government should minimize the burden on the private sector to report the same information through several channels, and the federal government should bear the burden of "connecting the dots" and communication among agencies.

Contacts

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

Ken D. Kumayama
Partner / Palo Alto
650.470.4553
ken.kumayama@skadden.com

Resa K. Schlossberg
Partner / New York
212.735.3467
resa.schlossberg@skadden.com

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

Jordan Cannon
Associate / Washington, D.C.
202.371.7542
jordan.cannon@skadden.com

Stephen A. Floyd
Associate / Washington, D.C.
202.371.7145
stephen.floyd@skadden.com

Joe Molosky
Associate / Chicago
312.407.0512
joe.molosky@skadden.com