wiley

ALERT

DHS Calls for Critical Harmonization of Cyber Incident Reporting

September 26, 2023

On September 19, 2023, the Department of Homeland Security (DHS) released a Report to Congress (Report) on the Harmonization of Cyber Incident Reporting to the Federal Government. The Report reflects on the 52 in-effect or proposed federal cyber incident reporting requirements that contribute to an inefficient patchwork of cybersecurity rules and proposals. A flurry of cyber activity has increased the urgency to harmonize and address the potential for duplicative regulations arising from current and future incident reporting regimes.

Congress directed DHS to create the Cyber Incident Reporting Council (CIRC), in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), which also directed DHS's Cybersecurity and Infrastructure Security Agency (CISA) to create broad new cybersecurity incident reporting mandates for the private sector. Congress recognized that the new mandatory reporting rules are likely to add to an already complex and fragmented reporting landscape, so CIRC was directed to review duplicative and burdensome reporting requirements and make recommendations for harmonization. The CIRC conducted the information collection and analysis included in the Report, to which dozens of companies and associations contributed.

As directed, the Report includes (1) a list of duplicative federal cyber incident reporting requirements on covered entities; (2) a description of any challenges in harmonizing the duplicative reporting requirements; (3) any actions the Director intends to take to facilitate harmonizing the duplicative reporting requirements; and (4) any proposed legislative changes necessary to address the duplicative reporting.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Lauren N. Lerman
Associate
202.719.4664
llerman@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

The Report is the most recent action addressing the need for cybersecurity reporting harmonization. It follows the Request for Information on Cyber Regulatory Harmonization released by the White House Office of the National Cyber Director (ONCD) on July 19, 2023. ONCD has extended the previous September deadline for comments to October 31, 2023.

Below we summarize key findings and recommendations in the Report.

Duplicative Federal Cyber Incident Reporting Requirements

CISA defined "duplicative reporting" or "duplication" as "regulatory requirements for the same reporting entity to report the same incident to more than one federal agency." After analyzing the federal cyber incident reporting requirements imposed by 22 different federal agencies, CISA found:

- 45 requirements are currently in effect and several more requirements are in the rulemaking process.
- While reporting incidents to government bodies provide national security, consumer protection, and public safety benefits, the patchwork of disparate requirements has led to the collection of the same information for the same cyber incidents.
- Duplicative reporting exists in industry-specific sectors. For example, in the communications sector, some entities are subject to two FCC reporting requirements for the same incident.
- Duplication also exists in cross-sector reporting where entities are subject to industry-specific rules as well as topical rules that are designed to provide specific information to specific parties.

The Report briefly flagged the additional burden of state breach notification laws.

Challenges in Harmonizing Duplicative Reporting Requirements

The Report identified four challenges in harmonizing duplicative reporting requirements: (1) Definitions; (2) Timelines and Triggers; (3) Content of Reports; and (4) Reporting Mechanisms.

Definitions. CISA observed that the terminology used to describe the impact of an event varied across reporting requirements. Terms such as "substantial loss," "disruption," and "serious impact" are all used to trigger reporting requirements yet are interpreted differently by different agencies. Similarly, regulatory agencies do not agree on whether ongoing internal investigations are considered "cyber incidents."

Timelines and Triggers. The timeline between the end of the cyber incident and when a report or notification is due varies from one hour to 60 days and sometimes includes vague terms such as "without delay" or "promptly."

Reporting Mechanisms. Different agencies require specific reporting mechanisms such as reporting via web forms, web portals, secure file transmission systems, or forms submitted via email. The variance between these formats requires extra work for entities reporting the same information to different agencies.

CISA Actions and Recommendations to Facilitate Harmonizing the Duplicative Reporting Requirements

The Report offers eight recommendations that the Federal Government could adopt to begin harmonizing duplicative cyber incident reporting.

Recommendation 1: Model Definition of a Reportable Cyber Incident. The Federal Government should adopt a model definition of "reportable cyber incident," applicable to multiple sectors. The model definition would exclude data breach reporting requirements.

The model definition proposed in the Report defines reportable cyber incident as a cyber incident that leads to or could reasonably lead to (1) a substantial loss of confidentiality, integrity, or availability of a network, (2) a disruption or significant adverse impact on the ability to engage in business operations or deliver goods and services, (3) disclosure or unauthorized access directly or indirectly to non-public personal information of a significant number of individuals; or (4) potential operational disruption to other critical infrastructure systems or assets.

Recommendation 2: Model Incident Reporting Timelines and Triggers. The Federal Government should adopt a model for reporting timelines and triggers. Agencies should include objective criteria to describe when a reporting obligation is triggered. Additionally, timelines for notification should be appropriate to allow the entities to determine the full impact of the incident and correctly identify the individuals who should be notified.

The model timeline outlined in the Report requires a covered entity to report the incident within 72 hours of a reportable cyber event, noting that incidents that disrupt national critical functions may require an entity to report sooner than 72 hours, and incidents involving loss of personal information without further impact on business operations may include a timeline longer than 72 hours.

Recommendation 3: Delay in Notifications where Security and Safety Involved. The Federal Government should adopt language that allows for delayed public notifications where notifying affected individuals may end up tipping off a bad actor during an active law enforcement investigation or national security risk.

The proposed model language in the Report allows for public disclosure to be delayed when the Attorney General or appropriate law enforcement official informs a covered entity that disclosure would pose significant risk. The delay may be extended for periods of up to 30 days pending a written request.

Recommendation 4: Adopt Model Reporting Form. CIRC member agencies should create a model form that could standardize the reporting process, especially in the initial reporting stages. This model form would also help with the eventual information sharing among agencies proposed in Recommendation 5.

Recommendation 5: Share Cyber Incident Reports and Information. Federal agencies should assess potential information sharing arrangements that could streamline the reporting process.

Recommendation 6: Allow Supplemental Reporting. Federal agencies should allow supplemental reporting or updates after a cyber incident is discovered. This flexibility can benefit entities and increase access to accurate information and the agencies' understanding of the incident.

Recommendation 7: Adopt Common Terminology. Terms such as "Initial Report" and "Notification" should be consistently used among agencies to have the same meaning to make it simpler for entities to know what is expected of them.

Recommendation 8: Improve Engagement with Entities. Agencies should coordinate with one another when engaging with the reporting entity to streamline communication and reduce the "potential for confusion, undue burden, or even distracting reporting entities that are in the midst of crisis from effective risk and consequence management."

Proposed Legislative Changes

The Report suggests that Congress (1) remove legal or statutory barriers to the creation of this cyber incident reporting harmonization; (2) provide funding and authority to agencies to collect and share cyber incident data; and (3) exempt cyber incident reporting from the Freedom of Information Act (FOIA).

Takeaways

The Report offers a first, but hopeful, step towards harmonizing the fragmented landscape of cybersecurity regulations. Moving forward, CIRC will support CISA in its efforts to review regulatory requirements and ensure reporting requirements are not necessarily duplicative.

Through streamlining duplicative and inconsistent reporting requirements, agencies, organizations, and consumers will benefit from lighter compliance burdens and greater national security protection.

Unfortunately, the Report may be too late to affect several developments, including controversial new obligations created by the Securities and Exchange Commission that mandate public disclosures of certain incidents in a manner and at a time that is at odds with the majority of other reporting approaches, including those commanded by Congress in CIRCIA.

The government has a separate proceeding underway to consider harmonization of affirmative cyber regulations, separate from incident reporting. Stakeholders are encouraged to address the benefits of such harmonization by filing a comment to the ONCD by October 31, 2023.

***

Wiley's Privacy, Cyber & Data Governance Team has helped companies of all sizes from various sectors proactively address risks and address compliance with new cybersecurity laws and requirements. Our team has been actively involved in almost every proceeding that is referenced in the Strategy and is advising clients on the likely results of new legislation, revisions to core NIST documents, and agency regulatory and oversight activities. Please reach out to any of the authors with questions.

Kimberly Alli, a Law Clerk in the Telecom, Media & Technology practice, contributed to this alert.