Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

Harmonic Dissonance—Synching Up Cybersecurity Regulations

July 31, 2023

On July 19, 2023, the Office of the National Cyber Director (ONCD) announced that it will start a process to harmonize cybersecurity regulations and seek regulatory reciprocity. In this pursuit, the White House released a Request for Information (RFI) seeking input from stakeholders on the regulations their industries and entities face, challenges they encounter in meeting those regulations, and potential gaps that exist.

This endeavor initiates an objective from the March 2023 *National Cybersecurity Strategy* and its implementation plan.

Efforts surrounding regulatory harmonization have been lauded by some Members of Congress and explored by congressional committees in the past. Yet, attempts to achieve regulatory alignment have been fruitless. Even after the ONCD's announcement, the Securities and Exchange Commission (SEC) announced that it adopted a new rule requiring publicly traded companies to disclose cybersecurity incidents to investors. This action front-runs similar disclosure rules that the Cybersecurity and Infrastructure Security Agency (CISA) is required to issue per the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), but are still in development.

This Insight discusses cybersecurity regulations, their harmonization, and options for Congress.

Cybersecurity Regulations

Prior to CIRCIA, the U.S. government did not have broadly applicable cybersecurity regulations. Instead, Congress and agencies established rules for cybersecurity sectorally—that is, agencies regulated specific sectors independently for specific purposes. Some, but not all, sectors are regulated for cybersecurity in some way. Most common among these regulations is the requirement to report incidents. For example, defense contractors, bulk electric system providers, financial depository institutions, health care facilities, nuclear power licensees, and transportation facilities all have responsibilities to report to a federal agency (or approved entity) when they experience cyber incidents. Some of these entities also have requirements for planning cybersecurity response activities, implementing mitigation strategies, and assigning responsibilities for cybersecurity to a facility's officer.

Congressional Research Service
https://crsreports.congress.gov
IN12211

The SEC rule is unique in the breadth of its applicability—all publicly traded companies, regardless of sector or other reporting requirements. The SEC's view is that cybersecurity risk must be assessed and disclosed to investors and that cyber incidents constitute material events. Previously, cybersecurity incidents were not largely considered material events, with a handful of incidents meeting that threshold (e.g., the Equifax Breach). The SEC's rule creates repetitive reporting requirements with the pending CIRCIA and existing sectoral rules.

In addition to federal regulation, private sector companies are also subject to numerous rules imposed by state regulatory agencies. There is no obligation for regulatory agencies to coordinate or deconflict their efforts, leading to some frustration within firms.

Individual entities may concurrently be subject to the CIRCIA rule, SEC rules, and sectoral rules. These requirements may compel the same information to be repeatedly disclosed to different regulators. The costs associated with regulatory compliance have been cited by some industry groups as burdensome.

Harmonizing Regulations

Recognizing the challenges in harmonizing regulations, the ONCD is pursuing a variety of options. The RFI is open for public comment until mid-September 2023, and ONCD officials have suggested that harmonization efforts will be a multi-year process. First, the ONCD plans to solicit feedback and develop a framework for regulatory harmonization. Two framework options the ONCD is already considering are the application of regulations in a tiered manner (e.g., aligning requirements to existing business size to allow small and medium businesses flexibility) and pursing reciprocity among agencies for issued regulations (rather than attempting to harmonize those regulations).

In its March 2020 report, the Cyberspace Solarium Commission acknowledged the tension between burdensome regulations and the utility of regulations in improving cybersecurity outcomes. Ultimately, the Commission did not make a recommendation regarding harmonization, partly because of the challenges in doing so.

Councils for pursuing regulatory harmonization existed prior to and after the Commission's review. In both cases, noticeable progress towards harmonization have not been publicly observed or achieved.

- The Cybersecurity Forum for Independent and Executive Branch Regulators existed before the Commission. According to its charter, the body, then chaired by the Nuclear Regulatory Commission, sought to "increase the overall effectiveness and consistency of regulatory authorities' cybersecurity efforts." It has since been revitalized under the leadership of the Federal Communications Commission.
- The National Cybersecurity Strategy proposes using the CIRCIA-created Cyber Incident Reporting Council (CIRC) to coordinate and advance common standards and deconflict the variety of federal cyber incident reporting requirements. While this is a responsibility given to the CIRC in its authorizing legislation, the law does not provide new regulatory authority, nor does it extend to other cybersecurity regulations (e.g., minimum standards and planning requirements).

Considerations for Congress

After Congress determines that a regulation is needed, authority to regulate is usually granted in a three-step framework. First, an authorized entity would *create* the regulation which industry must follow. This is also called *rulemaking*. Next, an agency could *examine* or *supervise* for compliance with the regulation. If a company is found to be not in compliance with the regulation, an agency could *enforce* the regulation (e.g., suing the company or issuing a fine). Congress may grant authority to different agencies for each

step in this framework. Critical to this framework is that regulation be independent of other agency authorities and activities.

Regulatory independence has been a key tenet of rulemaking, but also contributes to challenges in achieving harmonization. It is unclear what requirement or incentive that regulatory agencies have to issue, alter, or remove regulations to align with another's.

Congress may choose to monitor these harmonization efforts in an effort to oversee their success. Congress may face a question of granting new and explicit authorities for issuing regulations or directing an agency to change existing regulations. Congress may also choose to explicitly authorize an office, agency, or council with the responsibility for ensuring that cybersecurity regulations are harmonized (or reciprocal) and empowering that body with the authorities necessary to ensure that it can happen. Congress can also choose to direct regulatory agencies to change their regulations to harmonize or reciprocate with others.

In pursuing any of these options, current ONCD efforts to explore harmonization could inform future congressional action.

Author Information

Chris Jaikaran
Specialist in Cybersecurity Policy

Disclaimer