wiley

ALERT

Biden Administration Looks at Harmonizing Cyber Regulations Amidst Flurry of New Activity

August 3, 2023

Cybersecurity continues to be top of mind for federal and state policymakers. This advisory identifies and analyzes some major recent developments that present opportunities and challenges in the coming months for a broad swath of private sector organizations.

Just in the past several months, a variety of new cybersecurity proposals, taskforces, and legislative efforts have been put forward—from sector-specific cybersecurity efforts to cyber incident reporting obligations for all public companies, with more on the horizon. These latest developments add to an already crowded field of various federal and state efforts and requirements. In recognition of the inherent problems with such a fragmented approach, Congress created the Office of the National Cyber Director (ONCD) within the Executive Office of the President to coordinate cybersecurity policy and strategy. ONCD is taking the lead on coordinating implementation of the White House's National Cybersecurity Strategy and as part of that effort, ONCD recently released a request for information (RFI) that seeks comment on how to harmonize cybersecurity regulations.

Below we discuss some of the new cybersecurity rules and proposals issued in the past few months and provide additional details about ONCD's RFI. For organizations that are contending with the growing patchwork of federal and state cybersecurity requirements, this continued fragmentation is troubling, but the federal effort towards harmonization is promising. Stakeholders who would like to weigh in with ONCD have until **September 15, 2023** to file comments.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kara M. Sacilotto
Partner
202.719.7107
ksacilotto@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
jfbrown@wiley.law

Lauren N. Lerman
Associate
202.719.4664
llerman@wiley.law

Practice Areas

Artificial Intelligence (AI)
Cybersecurity
Federal Policy and Regulation
Government Contracts
Government Contracts
Litigation
Privacy, Cyber & Data Governance
Securities Enforcement and Litigation

Recent Federal Cybersecurity Activity

SEC Cybersecurity Rule. On July 26, 2023, the U.S. Securities and Exchange Commission (SEC) approved a final rule in its Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure proceeding. The vote came after the SEC's March 2022 Notice of Proposed Rulemaking (NPRM), which generated robust stakeholder engagement. The SEC received over 150 comments, many of which were heavily critical of key elements of the proposal given the myriad of other cyber obligations faced by diverse public companies. Despite these concerns, the SEC explained, in the final rule, that the impetus behind the new rule is the economy's increasing dependence "on electronic systems, such that disruptions to those systems can have significant effects on registrants," and the rise in major cybersecurity incidents in recent years. The SEC Commission further noted that although existing rules require disclosure of information about material events and cyber risks, there are no specific guidelines for where or how companies are supposed to report cybersecurity incidents in SEC filings, which the SEC claims makes it "difficult for investors to locate, interpret, and analyze the information provided."

At a high level, the final rule requires: (1) disclosure of a material cybersecurity incident on Form 8-K; and (2) additional disclosures of cyber risk management, strategy, and governance on Form 10-K. The new rule amends Form 8-K to require SEC registrants to disclose any cybersecurity incident within 4 days of determining that the incident is material. The disclosure must include: (1) material facts related to the nature, scope, and timing of the incident; and (2) what material impact or reasonably likely material impact will result from the incident (e.g., strained financial condition and compromised operations). The rule similarly amends Form 10-K to require periodic disclosure of cybersecurity risk management, strategy, and governance.

The rule will become effective 30 days after Federal Register publication, but the SEC lays out additional timelines for the various requirements within the rule. Specifically:

- The requirement to describe the company's cyber risk management, strategy, and governance will be effective December 15, 2023.
- The incident disclosure requirement will be effective the latter of: (1) December 18, 2023; or (2) 90 days after Federal Register publication. Smaller companies must comply with the incident disclosure requirement the latter of (1) June 15, 2024; or (2) 270 days after Federal Register publication.

This new rule is part of a growing trend towards incident reporting expectations, including a broad new incident reporting obligation on critical infrastructure under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)—for which the U.S. Department of Homeland Security (DHS) is in the process of developing new rules—as well as proposed updates to the New York Department of Financial Service's Cybersecurity Rules.

TSA Updated Pipeline Cybersecurity Directive. Also on July 26, 2023, the Transportation Security Administration (TSA) updated its Security Directive, first issued in July 2021, with updates for the preventative cybersecurity practices of oil and gas pipelines. In general, this Directive is designed to strengthen the resiliency of the oil and gas pipelines to avoid cyber attacks similar to the one on Colonial Pipeline two years

ago that is widely considered a watershed moment in cybersecurity. The updated Directive still requires pipeline owners and operators to comply with the existing "performance-based regulatory cybersecurity measures," and adds three new requirements:

- Owners' and operators' annual Cybersecurity Assessment Plans now need TSA approval, extending beyond the previous requirement that the plans merely be submitted for review;
- All cybersecurity measures will need to be tested every three years, so annual reports must include the results of such prior assessments and schedules for when new testing of those cybersecurity measures will take place; and
- Two of the Cybersecurity Incident Response Plan objectives must be tested annually and the employees who participate in those tests need to be identified in the annual report.

DOD Cybersecurity Maturity Model Certification. On July 24, 2023, the long-awaited U.S. Department of Defense (DOD) Cybersecurity Maturity Model Certification (CMMC) program proposed rule advanced to the Office of Management and Budget's Office of Information and Regulatory Affairs (OIRA) for review. OIRA has 90 days to conduct its review, although nothing precludes OIRA from taking longer. If OIRA does not return the regulation to DOD to address findings from OIRA's review, the next step is publication of the CMMC proposed rule in the Federal Register in or around late September. The OIRA dashboard and other previous CMMC artifacts indicate the rulemaking is in the form of a proposed rule and consequently, the public will have an opportunity to provide comment before CMMC, in some form, takes effect.

By way of background, CMMC as a concept was introduced in May 2019. In September 2020, DoD published an interim Defense Federal Acquisition Regulation Supplement (DFARS) rule to implement its initial version of CMMC, dubbed CMMC 1.0, which included (i) five levels of standards, depending on the sensitivity of the data to which the contractor had access, (ii) third-party assessments of whether the contractor's cybersecurity controls met a particular level, and (iii) implementation through solicitations and contractual clauses. The interim rule became effective on November 30, 2020, but it was short-lived. In March 2021, DoD initiated a reassessment of the CMMC program based on public input on CMMC 1.0, and in November 2021, it announced an updated CMMC program, CMMC 2.0, which would be rolled out in its own rulemaking and made significant changes to the CMMC model. It also suspended CMMC pilot efforts and inclusion of CMMC in new solicitations.

The broad contours of CMMC 2.0 have been available on the DoD Chief Information Officer website (with a large yellow note warning that the site will not be updated during the rulemaking process). With CMMC 2.0 at OIRA, the wait for a more detailed look at the revised program appears to be coming to a close. Release of a proposed rule in fall 2023 would align with DoD's desire to include the new requirements in contracts by fall 2024.

FCC Privacy and Data Protection Task Force. In a June 14, 2023 speech, Federal Communications Commission (FCC or Commission) Chairwoman Jessica Rosenworcel announced that the FCC is launching a new, "first-ever" "Privacy and Data Protection Task Force" (Task Force). Emphasizing that the FCC "has an important role to play in ensuring the privacy of consumer communications" and that it needs to "concentrate

[its] efforts" on the "magnitude of privacy challenges we face," the Chairwoman explained that the Task Force will bring "technical and legal experts together from across the agency to maximize coordination and use the law to get results—by evolving [the agency's] policies and taking enforcement action."

According to the press release announcing its launch, the Task Force is an FCC staff working group that will "coordinate across the agency on the rulemaking, enforcement, and public awareness needs in the privacy and data protection sectors." Those needs are described by the Task Force to include "data breaches – such as those involving telecommunications providers and related to cyber intrusions – and supply chain vulnerabilities involving third-party vendors that service regulated communications providers."

Since the June launch, the Task Force announced on July 11, 2023, that Chairwoman Rosenworcel has circulated for her fellow Commissioners' review new rules in the FCC's ongoing proceeding to "protect consumers from scammers who target data and personal information through SIM swapping scams and port-out fraud."

Federal Information Security Modernization Act of 2023. Finally, there have been updates from Congress as well. On July 12, 2023, the Federal Information Security Modernization Act (FISMA) of 2023, S. 2251, was introduced in the Senate by Committee on Homeland Security and Governmental Affairs (SHSGAC) Chairman Gary Peters (D-MI), and Sen. Josh Hawley (R-MO). A House version of the bill, H.R. 4552, was introduced by Rep. James Comer (R-KY), chairman of the House Oversight and Reform Committee (House Oversight); Rep. Nancy Mace (R-SC), chairwoman of the Cybersecurity, Information Technology, and Government Innovation subcommittee; Rep. Gerry Connolly (D-VA), ranking member of the subcommittee; and Rep. Jamie Raskin (D-MD), ranking member on House Oversight. On July 26, 2023, SHSGAC advanced the bill.

FISMA was originally passed in 2002. In 2014, Congress amended FISMA to modernize federal security practices to address evolving security concerns. Further updates have been expected, with renewed interest arising from the increasing frequency of data breaches and other cybersecurity incidents involving federal information systems.

The current bill includes provisions to support more effective cybersecurity practices throughout the federal government; improve coordination between federal agencies and contractors in addressing cyber threats; and promote security principles and programs such as vulnerability disclosure programs, penetration testing, zero trust architectures, and the use of artificial intelligence (AI) in automation. The bill also proposes government contractor reporting of certain cybersecurity incidents and extends the reporting requirements into receipt of personally identifiable information (PII). Further, the bill includes several cybersecurity requirements for agencies as well, including cyber incident reporting requirements, and recommends implementation of cybersecurity measures such as penetration testing and zero-trust architecture.

While the bill promotes improved coordination between agencies and contractors in addressing cyber threats, it is unclear whether the projected incident reporting timeframes and definitions will align with other efforts related to safeguarding sensitive information, such as Controlled Unclassified Information (CUI), which already impose significant reporting requirements on contractors. Congress continues to debate the final version of

the bill, so it remains to be seen if or exactly what new obligations will be imposed on federal contractors.

ONCD Harmonization RFI

In the context of this increasingly fragmented legal and regulatory landscape, on July 19, 2023, as part of the Biden Administration's National Cybersecurity Strategy, ONCD released an RFI inviting public comment on opportunities for, and obstacles to, harmonizing federal cybersecurity regulations. Comments on the RFI are due by September 15, 2023.

The RFI builds on the commitment the Administration made in the National Cybersecurity Strategy to "harmonize not only regulations and rules, but also assessments and audits of regulated entities." Inconsistent, contradictory, or duplicative cybersecurity regulations, the Administration believes, can lead companies to focus more on compliance than security which results in passing higher costs on to customers and working families, as well as state and local governments. Harmonizing baseline regulatory requirements are seen by the Administration as a way to produce better security outcomes at lower costs.

ONCD is seeking input to help them understand the existing challenges with regulatory overlap and inconsistencies to help the government create a framework where regulators can reciprocally recognize common baseline requirements given technological commonalities among various sectors and entities. In the RFI, ONCD invites public comments on cybersecurity regulatory conflicts, inconsistencies, redundancies, challenges, and priorities in response to ten specific questions. ONCD is particularly interested in regulatory harmonization as it applies to critical infrastructure sectors and sub-sectors identified in Presidential Policy Directive (PPD)-21 and the National Infrastructure Protection Plan, and providers of communications services, IT services, or cybersecurity services to owners and operators of critical infrastructure. In this context, "harmonization" refers to a common set of updated baseline regulatory requirements that would apply across sectors. Sector regulators could still go beyond the harmonized baseline to address cybersecurity risks specific to their sectors. Keep in mind that the White House has also announced that it is seeking to "refresh" PPD-21 as the threat landscape has changed dramatically over the past decade.

ONCD strongly encourages industry associations, regulated entities, and others with expertise in cybersecurity regulation, risk management, operations, compliance, and economics to respond to this RFI. Highlights of questions for respondents in the RFI include:

- Examples of conflicting, mutually exclusive, or inconsistent regulations;
- Evaluations of the use of common guidelines;
- Comments on the use of existing standards or frameworks to achieve regulatory harmonization;
- Harmonizing regulations affecting cloud and other service providers;
- Examples of State, Local, Tribal, and Territorial regulations affecting critical infrastructure owners and operators across state lines; and
- Examples of international regulatory regimes that have overlapping, redundant, or inconsistent requirements.

Of note, ONCD has carved out incident reporting from its RFI, explaining that "[s]uch requirements are being analyzed through a separate effort led by the Cyber Incident Reporting Council established by the Secretary of Homeland Security as required by the Cyber Incident Reporting for Critical Infrastructure Act of 2022."

Key Takeaways

The continued onslaught of new cybersecurity proposals and expectations create complex compliance burdens on organizations across a range of sectors, many of whom are already subject to various other cyber incident reporting and regulatory obligations. As the number of cybersecurity laws and regulations are increasing, ONCD's RFI provides stakeholders with an opportunity to reiterate to the federal government the importance and benefits of harmonization.

***

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.