KPMG

Regulatory Alert

Regulatory Insights

June 2024

Cybersecurity Strategy: ONCD, GAO

KPMG Insights:

- ***Top Priority:*** *Concurrent issuances/actions from ONCD and GAO reiterate cyber as a top regulatory priority.*
- ***Harmonizing Cyber Regulations:*** *Recommendations and RFI related to potential for creating a 'unified cybersecurity framework', streamlining regulations, and establishing reciprocal recognition across critical infrastructure sectors while recognizing associated challenges.*
- ***Baseline Cyber Standards:*** *Desire for "baseline cybersecurity standards" across critical infrastructure sectors, that aim to reduce compliance costs.*

In furtherance of the National Cybersecurity Strategy announced by the White House in March 2023, the Office of the National Cyber Director (ONCD) and the General Accountability Office (GAO) each take steps to consider the challenges associated with establishing new and updated cybersecurity regulations and frameworks that are "tailored for each sector's risk profile," harmonized and streamlined to reduce duplication, and "calibrated to meet the needs of national security and public safety." These actions include a:

1. Summary Report of the ONCD Request for Information (RFI)
2. GAO Report, entitled "Cybersecurity: Efforts Initiated to Harmonize Regulations but Significant Work Remains"

Both the ONCD Summary Report and the GAO Report are covered in testimony before the United States Senate Committee on Homeland Security and Governmental Affairs at a recent hearing on "Streamlining the Federal Cybersecurity Regulatory Process: The Path to Harmonization."

1. ONCD RFI Summary

The ONCD, a component of the Executive Office of the President established to advise the President on cybersecurity policy and strategy, releases a Summary Report on comments received in response to its August 2023 RFI on cyber regulatory harmonization. (See related White House release, here.)

The ONCD, in coordination with the Office of Management and Budget, is tasked with leading the Administration's efforts on cybersecurity regulatory harmonization pursuant to the National Cybersecurity Strategy (see KPMG's Regulatory Alert, here). Responses to the RFI are intended to help the ONCD "understand existing challenges with regulatory overlap and explore a framework for reciprocity…in regulator acceptance of other regulators' recognition of compliance with baseline requirements." The ONCD states that it is "particularly interested in regulatory harmonization as it may apply to critical infrastructure sectors and sub-sectors…and providers of communications, IT, and cybersecurity services to owners and operators of critical infrastructure.

For these purposes:

- "Harmonization" refers to a common set of updated baseline regulatory requirements that would apply across sectors.
- "Reciprocity" means mutual recognition of compliance findings across regulations and/or jurisdictions.
- Baseline requirements would apply to all sectors and regulators; regulators could impose requirements

beyond the baseline requirements to capture unique sector-specific risks.

Eleven of the sixteen critical infrastructure sectors were among the respondents to the RFI. As identified in the Summary Report, key findings include:

- The lack of harmonization and reciprocity harms cybersecurity outcomes while increasing compliance costs through additional administrative burdens.
- Challenges with cybersecurity regulatory harmonization and reciprocity extend to businesses of all sectors and sizes and cross jurisdictional boundaries.
- The U.S. Government is positioned to act to address these challenges. Respondent recommendations include legislation to set national, high-level standards for cybersecurity, and ways to include independent regulators in future planning for regulatory harmonization.

Questions in the 2023 RFI focused on the following topics:

- Conflicting, mutually exclusive, or inconsistent regulations.
- Use of common guidelines (e.g., Federal Financial Institutions Examination Council (FFIEC)).
- Use of existing standards or frameworks.
- Third-party frameworks (e.g., NIST Cybersecurity Framework).
- Tiered regulation (e.g., risk-based regulatory requirements for sectors).
- Oversight by multiple regulators of the same entity.
- Cloud and other service providers.
- State, local, tribal, and territorial regulation.
- International regulation.

2. GAO Report

The GAO Report, "Cybersecurity: Efforts Initiated to Harmonize Regulations but Significant Work Remains," outlines the Administration's recent work to harmonize cybersecurity regulations, including the ONCD RFI. The efforts (other than the ONCD RFI) include release of the:

- National Cybersecurity Implementation Plan Version 2 (May 2024) containing initiatives to be completed by March 2025 or earlier, including:
  - Setting minimum cybersecurity requirements across critical infrastructure sectors.
  - Increasing agency use of frameworks and international standards to inform regulatory alignment. (Note: The National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 (February 2024) responds to this initiative.)
  - Exploring cybersecurity regulatory reciprocity pilot programs (Note: The National Cyber Director stated ONCD is working on a pilot program for regulatory reciprocity frameworks to be used in a critical infrastructure sub-sector and to provide insights into effective regulatory designs).
- National Security Memorandum on Critical Infrastructure Security and Resilience ("National Security Memorandum -22", April 2024), which calls for:
  - Federal department and agencies to use regulation to establish minimum requirements and accountability mechanisms for the security and resilience of critical infrastructure.
  - The Secretary of Homeland Security to prepare a report to the President by April 2025 and every two years thereafter on the National Infrastructure Risk Management Plan, which includes a plan for harmonizing minimum security and resilience requirements across all sectors.
- Cybersecurity and Infrastructure Security Agency (CISA) proposed rule on cyber incident and ransom payment reporting requirements for covered entities; CISA seeks comment on how to harmonize these requirements with other federal reporting regimes. (Comments due to CISA by July 3, 2024.)

The GAO Report also notes that challenges to harmonization across sectors include "differences in the:

- Definitions of reportable cyber incidents and thresholds for reporting.
- Timelines and triggers for reporting.
- Contents of incident reports.
- Reporting mechanisms.
- Procedural and resource burdens.
- Legal barriers and limits on agency authorities."

For more information, please contact Amy Matsuo or Matt Miller.

.

Contact the author:

Amy Matsuo
Principal and National Leader
Regulatory Insights
amatsuo@kpmg.com

kpmg.com/socialmedia