MITRE's Response to the ONCD RFI on Cybersecurity Regulatory Harmonization

October 31, 2023

For additional information about this response, please contact:

Duane Blackburn
Center for Data-Driven Policy
The MITRE Corporation
7596 Colshire Drive
McLean, VA 22102-7539

policy@mitre.org
(434) 964-5023

About MITRE

MITRE is a not-for-profit company that works in the public interest to tackle difficult problems that challenge the safety, stability, security, and well-being of our nation. We operate multiple Federally Funded Research and Development Centers (FFRDCs), participate in public-private partnerships across national security and civilian agency missions, and maintain an independent technology research program in areas such as artificial intelligence, intuitive data science, quantum information science, health informatics, policy and economic expertise, trustworthy autonomy, cyber threat sharing, and cyber resilience. MITRE's 10,000-plus employees work in the public interest to solve problems for a safer world, with scientific integrity being fundamental to our existence. We are prohibited from lobbying, do not develop or sell products, have no owners or shareholders, and do not compete with industry—allowing MITRE's efforts to be truly objective and data-driven. Our multidisciplinary teams (including engineers, scientists, data analysts, organizational change specialists, policy professionals, and more) are thus free to dig into problems from all angles, with no political or commercial pressures to influence our decision making, technical findings, or policy recommendations.

In responding to this Request for Information (RFI), MITRE is drawing from our independent research and sponsor-funded work with federal agencies that promulgate policy and guidance; public and private sector critical infrastructure owners/operators; industry vendors/providers of solutions and services to critical infrastructure owners/operators; and government, industry, and independent standards-setting organizations operating in the following critical infrastructure sectors:

- Chemical
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Energy
- Financial Services
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Transportation Systems
- Water and Wastewater

Introduction and Overarching Recommendations

As the Office of the National Cyber Director (ONCD) contemplates cybersecurity regulations to secure critical infrastructure, MITRE recommends that potential new, and/or refinements to existing, cybersecurity regulations not specify technical requirements or implementation details for critical infrastructure (CI) owners/operators or the industry vendors/providers that support them. Specifying such details would further complicate continuous regulation harmonization, and updates would likely not keep up with the rapidly evolving cybersecurity landscape.

Instead, we recommend regulations and/or administration guidance focus on providing Sector Risk Management Agencies (SRMAs) with additional direction on how to shift the focus from compliance checking to strengthening the mechanisms needed by CI owners/operators and the vendors/providers that support them to produce meaningful improvements and more consistent outcomes. These mechanisms are within the SRMA responsibilities identified in 6 USC 665d; however, the SRMAs could benefit from (a) direction to provide CI sector-specific risk-based self-assessments, specific improvements to vulnerability and threat data and information sharing, and CI sector-specific technical assistance, and (b) organizational capacity and expertise to successfully accomplish these activities.

SRMA support to individual CI sectors needs to be tailored to the specific needs of a CI sector, while also enabling cross-sector collaboration and understanding.

Individual sectors have sector-specific needs for which they are supported by SRMAs. To reduce all-hazards CI risk, there is a need for frameworks that enable each CI sector to self-evaluate its specific risks, identify specific improvements in vulnerability and threat data and information sharing, and provide CI sector-specific technical assistance. At the same time, as vulnerabilities and threats can cut across individual sectors, it is also important for this support to enable cross-sector sharing and understanding.

Frameworks to enable CI sectors to identify specific risks must:

- Integrate and tailor existing frameworks and standards for the specific CI sector.
- Provide CI owners/operators and industry vendors/providers with an ability to prioritize risk information and risk mitigation actions tailored for different categories of CI owners/operators and industry vendors/providers (e.g., small/medium/large-size organizations; local/regional/national operators).
- Inform the CI sector-specific information and data sharing structure and categorization.
- Incorporate relevant cross-sector requirements to inform cross-sector risk management.

CI sector-specific data and information sharing mechanisms, such as Information Sharing and Analyses Centers, must:

- Anonymize and protect sharable data and information in a manner that engenders the trust of CI owners/operators and industry vendors/providers.
- Push to CI owners/operators and industry vendors/providers prioritized data and information and prioritized mitigation actions tailored for different categories of CI owners/operators and industry vendors/providers.
- Provide data and information that informs updates to the framework that enables identification of CI-specific risks.
- Ensure anonymized CI sector-specific data and information is sharable with cross-sector information sharing entities to identify cross-sector risks.

The CI sector-specific technical assistance must:

- Provide CI owners/operators and vendors/providers high-quality, timely assistance in risk assessment and mitigation.
- Provide an appropriate level of CI sector-specific technical assistance tailored for different categories of CI owners/operators and industry vendors/providers.
- Enable analysis at speed and scale where possible.

SRMAs must have the organizational capacity and expertise to strengthen these three mechanisms needed by CI owners/operators and the vendors/providers that support them.

Based on the specific activities described above, the SRMAs, in consultation with the Cybersecurity and Infrastructure Security Agency (CISA), should identify the organizational capacity and expertise needed to successfully accomplish the activities. If additional funding is needed, the SRMAs should develop a funding request that can then be evaluated by the ONCD to support Office of Management and Budget (OMB) Resource Management Office budget proposals and decision making.

Evidence Supporting MITRE’s Overarching Recommendations

The recommendations MITRE is presenting above are based on MITRE’s long-standing independent research and extensive sponsor-funded work with federal agencies on cybersecurity issues; public and private sector critical infrastructure owners/operators; industry vendors/providers of solutions and services; and government, industry, and independent standards-setting organizations. MITRE’s recommendations in its RFI response are based on four (4) key observations and findings. Additional details are provided in our responses to selected questions in the next section of this RFI response.

First, there is a perception by CI owners/operators and industry vendors/providers that there are multiple existing standards, frameworks, and guidance. In particular, the numerosity and complexity of the requirements make it difficult for those who are not cyber experts to integrate information and be assured that all the cyber-related requirements are addressed. In addition, CI owners/operators and industry vendors/providers need specific guidance, tailored to their CI sector, to be able to understand and implement the requirements. The multiple standards, frameworks, and guidance are dispersed, rather than integrated in a manner that prioritizes the risks and mitigation actions in a meaningful way. Without explicit guidance on how to prioritize risks and mitigation actions, many CI stakeholders are unable to appropriately calibrate their resources to address the requirements. This and the perception that oversight and reporting organizations view these requirements as “check the box” compliance exercises misses the opportunity to have meaningful dialogue on critical risks to be addressed.

Second, while CI sectors have some data and information sharing mechanism(s) in place, across all CI sectors there are challenges with consistent access, sharing, and/or protection of the data. Specifically, rather than being pushed to CI owners/operators and industry vendors/providers, information sharing is often conducted by a “pull” model that requires CI owners/operators and industry vendors/providers to continuously check for information. This creates obstacles to CI owners/operators and industry vendors/providers across all sectors submitting timely and complete data and information. Also, the data and information are not consistently perceived to be sufficiently anonymized or protected. This poses concerns where data may be shared with all CI owners/operators and industry vendors/providers within a CI sector or between CI sectors.

Third, technical assistance for risk assessments and risk mitigation is available from government entities. There is a concern from some owners/operators about the timeliness of these products, with various departments and agencies currently working to improve the timeliness. There is also a continuous need for CI owners/operators and industry vendors/providers to receive more tailored technical assistance by CI sector and different categories of CI owners/operators and industry vendors/providers to facilitate successful implementation of the requirements.

Fourth, for individual SRMAs, there are opportunities to enhance overall capacity and expertise, as well as ensure the capacity and expertise are well-aligned within the organization to successfully accomplish the activities described above. For example, some agencies have SRMA responsibilities well-placed organizationally and sufficiently staffed, some have good placement but not enough well-versed staff, and others have both placement and staffing issues.

Response to Questions Posed in the RFI

1. Conflicting, mutually exclusive, or inconsistent regulations – If applicable, please provide examples of any conflicting, mutually exclusive, or inconsistent federal and State, local, tribal, and territorial (SLTT) regulations affecting cybersecurity – including broad enterprise-wide requirements or specific, targeted requirements – that apply to the same information technology (IT) or operational technology (OT) infrastructure of the same regulated entity. Be as clear, specific, and detailed as possible.

a. Please include specific examples with legal citations or hyperlinks to the particular federal or SLTT cybersecurity rules or enforceable guidance that impose conflicting, mutually exclusive, or inconsistent requirements, and explain the specific conflicts or inconsistencies you identify.

Below are four examples of inconsistent cybersecurity requirements within a sector:

Example 1: Financial Services Sector – Proposed rules by the Securities and Exchange Commission on reporting timelines and definitions of incident and significant incident[1] are inconsistent with the Federal Incident Reporting Requirements.[2]

Example 2: Water and Wastewater Sector – The Environmental Protection Agency put forth cybersecurity requirements in its Sanitary Surveys for public water systems to assess their cybersecurity practices and controls every three to five years using an adapted CISA Cybersecurity Performance Goals Checklist. These requirements apply to only drinking water systems, not wastewater systems.[3]

Example 3: Transportation Sector (Pipeline Systems) – The Transportation Security Agency (TSA) put forth cybersecurity requirements for oil and natural gas pipeline owners/operators to

[1] Proposed rule: Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents. 2023. U.S. Securities and Exchange Commission, https://www.sec.gov/rules/2023/03/cybersecurity-risk-management-rule-broker-dealers-clearing-agencies-major-security. Last accessed October 25, 2023.

[2] US-CERT Federal Incident Notification Guidelines. Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf.

[3] Drinking Water Requirements for States and Public Water Systems – Sanitary Surveys. 2022. United States Environmental Protection Agency, https://www.epa.gov/dwreginfo/sanitary-surveys. Last accessed October 25, 2023.

perform an annual assessment of their cybersecurity practices and controls but does not specify a standardized Cybersecurity Assessment Plan tool.[4]

Example 4: Transportation Sector (Rail Systems) – The TSA put forth cybersecurity requirements for surface transportation systems to perform four critical actions:

- Designate a cybersecurity coordinator,
- Report cybersecurity incidents to CISA,
- Develop a cybersecurity incident response plan, and
- Conduct a cybersecurity vulnerability assessment using a TSA-provided form.[5]

The rail systems cybersecurity requirements do not cover all types of rail (e.g., freight rail but not passenger rail) and are inconsistent with the pipeline systems cybersecurity requirements and with cybersecurity requirements for aviation systems.[6] In addition, the rail systems cybersecurity requirements do not require follow-up reporting or independent evaluation to ensure cybersecurity vulnerabilities are addressed.

The impact of these inconsistencies and gaps in cybersecurity requirements is that CI owners/operators within the same sector—most of whom do not have access to cyber experts—interpret, integrate, and extend the various cybersecurity requirements, which then results in inconsistent outcomes within a CI sector.

4. Third-Party Frameworks – Both the government (for example, through the National Institute of Standards and Technology [NIST] Cybersecurity Framework) and non-government third parties have developed frameworks and related resources that map cybersecurity standards and controls to cybersecurity outcomes. These frameworks and related resources have also been applied to map controls to regulatory requirements, including where requirements are leveled by multiple agencies.

a. Please identify such frameworks and related resources, both governmental and nongovernmental, currently in use with respect to mitigating cybersecurity risk.

b. How well do such frameworks and related resources work in practice to address disparate cybersecurity requirements.

The U.S. Federal Government (USG) has been using the NIST Risk Management Framework (RMF) (NIST Special Publication [SP] 800-37) to manage security and privacy risk to federal information systems and satisfy the requirements in the Federal Information Security Modernization Act of 2014 (FISMA), the Privacy Act of 1974, OMB policies, and Federal

[4] Renewal with revision to the Security Directive (SD) Pipeline-2021-02 Series: Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing. 2023. Transportation Security Administration, https://www.tsa.gov/sites/default/files/tsa-sd-pipeline-2021-02d-w-memo_07_27_2023.pdf.

[5] Enhancing Rail Cybersecurity. 2022. Transportation Security Administration, https://www.tsa.gov/sites/default/files/sd-1580-21-01a.pdf.

[6] TSA issues new cybersecurity requirements for airport and aircraft operators. 2023. Transportation Security Administration, https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft. Last accessed October 25, 2023.

Information Processing Standards, and other requirements. USG agencies and organizations have established internal procedures and policies to implement the RMF, which has had impacts that extended beyond security and privacy risk management to areas such as workforce training (e.g., job-specific role and responsibilities), auditing requirements, acquisition processes, and requirements levied on contractors. The NIST RMF primarily exists at the system and information levels and does not provide organizational strategic risk management guidance across systems or programs, which can result in potential gaps for such guidance. Although the NIST RMF is intended to focus on risk management, gaps in organizational strategic risk management can contribute to a perception of implementing the RMF with a "check the box" mentality for implementers, regulators, and auditors. This can contribute to the regulations and auditing requirements surrounding use and implementation of the NIST RMF to focus on compliance with RMF steps and controls that organizations are expected to implement for their systems based on their security categorization and associated baselines, versus risk management practices and safeguards that reflect factors such as mission, environment, and system purpose.

To help organizations determine gaps in current cybersecurity risk approaches and develop roadmaps to improvement, NIST developed the Cybersecurity Framework (CSF), which USG agencies have been required to use to manage cybersecurity risks since 2017 with the signing of Executive Order (EO) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. The CSF was originally developed as a voluntary framework for protecting critical infrastructure. NIST now acknowledges its wider role in supporting cybersecurity risk management for NIST and organizations that have a wide variety of missions, business objectives, resources, maturity needs, and timelines.

NIST, as a non-regulatory agency, has not created assessment criteria or regulations on how the CSF should be implemented in order to maintain flexible cybersecurity risk management among its broad user base in the U.S., and internationally.

Sectors are developing CSF Profiles, such as a Liquified Natural Gas Profile,[7] an Elections Infrastructure Profile,[8] and other Profiles published and/or developed by either a sector/industry/community or NIST.[9] Profiles provide community-level cybersecurity guidance based on the cybersecurity landscape in that context, and allow each organization flexibility to implement the Profile based on its specific risks, threats, vulnerabilities, risk tolerances, resources, and activities. For those Profiles where NIST leads development, NIST has done so in collaboration and coordination with the community the Profile is intended for use by. With the pending 2.0 update to the NIST CSF, CSF Community Profiles (the official term for Profiles developed by a specific community such as the financial sector) are intended to further bring these communities together to collectively provide strategic cybersecurity guidance.

Once EO 13800 made the CSF mandatory for the USG to manage agency cybersecurity risk, the challenge was whether it replaced existing risk management processes, specifically the NIST RMF used widely by the USG. NIST developed the CSF with the flexibility to pair with existing business processes and risk management frameworks, including the NIST RMF. The CSF and

[7] Cybersecurity Framework Profile for Liquefied Natural Gas. 2023. National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8406-upd1.pdf.

[8] Cybersecurity Framework Election Infrastructure Profile. 2021. National Institute of Standards and Technology, https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8310-draft.pdf.

[9] Examples of Framework Profiles. 2023. National Institute of Standards and Technology, https://www.nist.gov/cyberframework/examples-framework-profiles. Last accessed October 25, 2023.

RMF pair well as complementary tools for holistically addressing risk management within an organization (among executive leadership, business operations, implementations/operations) and externally with partners. However, the USG is still working to understand how existing frameworks it has implemented (e.g., the NIST RMF) can be paired and intended to work with the CSF. The CSF and RMF, individually and collectively, can play a role in the holistic cybersecurity "toolkit" and minimize the likelihood of the frameworks being implemented inappropriately (e.g., at the system level, "checklist-ified"). Additionally, while use of frameworks such as the NIST RMF and CSF are required for use by the USG, they are not required for use by SLTT entities. While SLTT entities can be encouraged to use these frameworks by the USG, especially in situations where SLTT entities and USG agencies work in close collaboration with each other, use is typically voluntary and without the weight of regulations to require it.

Other frameworks that the USG uses to varying degrees include the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework, and threat frameworks such as MITRE ATT&CK®[10].

Frameworks like NIST's CSF and RMF and the other frameworks mentioned above were specifically designed to support cybersecurity risk management objectives and goals that can be achieved through individual use of the framework. Collectively, the frameworks are intended to provide a hierarchical approach to achieving cybersecurity goals at all levels within an organization from the senior leadership level to the information system level. With the introduction of new frameworks, including the NIST Privacy Framework and the Artificial Intelligence (AI) RMF, and the expectation of use comes the challenge of providing guidance, not regulations, on how these frameworks are intended to be used together as complements and not duplications of cybersecurity risk management activities, creating "framework fatigue" or unnecessary burdening of resources without enabling actual informed risk management decision making.

7. Cloud and Other Service Providers – Information technology, as a sector, is not regulated directly by the Federal government. However, regulated entities' use of cloud and other service provider infrastructure is often regulated. To date, regulators have typically not directly regulated cloud providers operating in their sector. Rather, regulatory agencies have imposed obligations on their regulated entities that are passed along by contract to the cloud provider/service provider.

a. Please provide specific examples of conflicting, mutually exclusive, or inconsistent cybersecurity regulatory requirements that are passed along by contract to third-party service providers.

Cybersecurity solutions are constantly evolving and Zero Trust principles are the latest paradigm for improving overall IT security especially when operating in the cloud. Based on MITRE's experience working with USG agencies and commercial cloud service providers (CSPs), we have observed the following gaps in CSP cybersecurity requirements:

[10] ATT&CK. 2023. MITRE, https://attack.mitre.org/. Last accessed October 30, 2023.

- CSPs are asked to comply with cybersecurity programs enforced by multiple government policy or regulatory structures, including FedRAMP (USG), FedRAMP+ (DoD), FedRAMP Accelerator (Intelligence Community), FAR/DFAR, NIST SP 800-171, RMF, FISMA, ITAR, HIPAA, and others. Each addresses a particular aspect of security, often for a specified domain. However, viewed collectively, gaps, overlaps, and conflicts exist. Many times, these various structures are implemented in differing ways through contracting vehicles. Examples include the multiple variations in security control baselines, or implied control baselines, across the various policy structures. A standardized federal government cybersecurity policy, having clear explanations for CSP compliance requirements, would be beneficial for simultaneously reducing gaps, overlaps, and conflicts, and reducing costs.

- Cybersecurity reporting by CSPs has not been standardized through government guidance. As a result, the timeliness and content of associated reporting is not consistent across CSPs. Standardization in what should be reported, and when, would be beneficial for the effective development and timely sharing of Cyber Threat Intelligence. For example, guidance regarding when to issue reports coupled with a data exchange standard similar to Fast Healthcare Interoperability Resources but focused on the requirements for threat monitoring and incident response reporting by CSPs would be beneficial. Such standards promote the transparent exchange of cybersecurity information across government and industry. Within the vein of the "shared responsibility model," associated disclosures should be made available to USG customers of CSPs. Cyber reporting should be both routine and near-real-time for specific incidents. Specific areas that should be included in routine disclosures and standard reporting include plans and status of:
    - Threat monitoring and incident response
    - Insider threat programs
    - Supply Chain Risk Management

- EO 14028[11] is driving the implementation of Zero Trust strategies for USG cybersecurity. However, associated cybersecurity requirements have not been included in agency acquisitions nor required of CSPs. All USG agencies should require the use of Zero Trust cybersecurity principles and application of the NIST SP 800-207 standard for all cloud service-based IT acquisitions. This will require the assessment of CSP Zero Trust Architectures and implementation solutions by FedRAMP and Agency Assessment and Authorization organizations.

[11] Executive Order on Improving the Nation's Cybersecurity. 2021. The White House, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/. Last accessed October 30, 2023.