October 19, 2023

Office of the National Cyber Director
Executive Office of the President
The White House
1600 Pennsylvania Ave. NW
Washington, DC 20500

RE: Response to Request for Information on Cybersecurity Regulatory Harmonization
Prepared by Charlie Tupitza, Director, Fusion3 Consulting

10. Additional Matters—Please provide any additional comments or raise additional matters you feel relevant that are not in response to the above questions.

Considering the Value of Harmonizing All Regulations

The enclosed considerations raise additional matters I feel relevant that are not in response to questions found in this request for information. They are from my long-term experience as a Cyber Resilience and IT Service Management professional. I was a charter member of Presidential Policy Directive 21 Cybersecurity working group for Critical Infrastructure, former US Head of Cyber Resilience for AXELOS (ITIL). As the Lead Cyber and Data Protection Consultant to the CEO of Americas Small Business Development Centers, I observed the impact of overlapping regulations on small and large businesses. For the past ten years I have been a member of the Critical Infrastructure Cybersecurity Forum, and active participant in the Software and Supply Chain Assurance Forum hosted by the DoD, GSA, DHS, and NIST.
I am a ServiceNow Certified Integrated Risk Management and GRC Implementation Specialist and have been actively engaged with the Cyber Security Maturity Model Certification (CMMC) and many NIST special publications and frameworks.

The National Cybersecurity Strategy 2023 calls out the Need to Harmonize Regulations

www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

"*Where feasible, regulators should work to harmonize not only regulations and rules, but also assessments and audits of regulated entities.****" …***

"Where Federal regulations are in conflict, duplicative, or overly burdensome, regulators must work together to minimize these harms."

Overlapping regulations are a problem to be addressed by the government in cooperation with regulated organizations to be effective and efficient. In the meantime, we all must take advantage of the opportunity to improve our risk posture through automation and best practices.

The Scope for Harmonization Considerations Needs to be Expanded

Since this effort is being addressed by the Office of the National Cyber Director at the White House, consideration should be given to the expansion of the scope to harmonize all federal regulations. Our National Cybersecurity Strategy states that we "*must be cognizant of the cost of implementation*." Overlapping of any regulation results in unnecessary costs.

It is inefficient to consider the management of Cybersecurity on its own. Software platforms, lessons learned, and best practices are available for public and private organizations to manage all risks with a level of continuity. Continuity is key to the reduction of financial costs and resources needed. Continuity is aided by a single source of truth associated with these platforms.

Cybersecurity regulations have direct relationships with many other regulations. Other regulations also overlap within their own domain putting an additional burden on organizations to manage risks efficiently and effectively.

Health and Human Services Recognizes Need for Harmonization of Regulations Broadly

The Immediate Office of the Secretary (IOS) at the Health and Human Services, issued a policy regarding redundant, overlapping, or inconsistent regulations on November 27, 2020. This Language is useful to assist other in this effort to harmonize regulations. *See Attachment A*

"Effective immediately, all agencies and offices of the Department that ***prepare regulations must ensure that any rule is not inconsistent with, and does not overlap with, any regulation that has already been issued*** *through an agency within the Department. In the event an agency proposing that the Secretary issue a rule discovers that such rule is inconsistent or overlaps with another Department rule, the proposing agency shall not recommend issuance until it also recommends to the Secretary the steps to be taken to avoid duplicative or overlapping regulations."*

The Federal Greenbook Recognizes Some Organizations Will Set Higher Objectives

Organizations will need to manage harmonization associated with their own objectives and regulations coming from the outside.

Find the Federal Green Book here: https://www.gao.gov/assets/gao-14-704g.pdf

"OV2.23 *Management conducts activities in accordance with applicable laws and regulations. As part of specifying compliance objectives, the entity determines which laws and regulations apply to the entity. Management is expected to set objectives that incorporate these requirements.* ***Some entities may set objectives to a higher level of performance than established by laws and regulations. In setting those objectives, management can exercise discretion relative to the performance of the entity."***

Additional Impact:

Federal regulations do not stand alone. Regulated organizations find themselves struggling to internally harmonize state, local, tribal, and other sources of regulations, especially from within Critical Infrastructure Sector communities and from others within the organization's business ecosystem.

Environmental, Social, and Governance (ESG) regulations misaligned with organizational values and understandings may also affect performance. These overlaps impact the public and private sectors.

There will always be a harmonization burden since overlaps exist beyond regulatory demands. All organizations, including the government, have a need to address harmonization as a continual improvement process.

Value of Automation:

The **automation capabilities of Integrated Risk Management** significantly enhance our ability to monitor/manage the overall risks of the organization to help ensure regulatory compliance. This technology encourages active involvement from **all stakeholders**, promoting a collective effort in risk reduction. It also ensures smooth continuity across all risk management activities, leading to increased efficiency and more reliable outcomes.

Additionally, incorporating Regulatory Harmonization as a Service further boosts the efficiency and effectiveness of automation within Integrated Risk platforms. Tailored automated reports are provided to **Board Members and Senior Executives,** supporting their crucial roles in overseeing comprehensive risk management.

Automation expands the influence of **Dedicated Risk Managers** by taking advantage of the single source of truth across all risks.

Subject matter experts in risk domains can now communicate their insights with precision, benefiting the highest levels of governance. This streamlined communication enables risks to be managed with clarity and transparency, providing senior stakeholders with the confidence they need.

Practitioners deeply involved in day-to-day risk management operations find automation to be a valuable ally. It simplifies their tasks and empowers them to effectively communicate their needs to senior executives, ensuring they have the necessary resources and support for their essential work.

Thank you for the opportunity to contribute. Please let me know if there is anything I can do to support this important effort. This is not a solicitation for business.

Regards,

Charlie Tupitza
Director
Fusion3 Consulting
https://www.Fusion3Consulting.com
https://www.linkedin.com/in/charlie-tupitza-009b4912/

ATTACHMENT A

Example of Regulatory Authority Recognizing and Acting on this Situation.

AGENCY: Immediate Office of the Secretary, Department of Health and Human Services (HHS).

ACTION: Policy statement.

SUMMARY: The Immediate Office of the Secretary (IOS) is issuing this policy regarding redundant, overlapping, or inconsistent regulations.

DATES: November 27, 2020.

The Department believes that its decision-making ought to be transparent, rational, and well-honed to achieve legitimate government objectives with minimum transaction costs to the affected sector. This policy furthers those objectives and the objectives of the Richardson Waiver (see 36 FR 2532 (Feb. 5, 1971)), and various Executive Orders by requiring that all regulations issued by this Department are necessary, understandable, and provide clear guidance to the public and regulated entities regarding the standards to be met and procedures to be followed. Redundant, overlapping, or inconsistent regulations undermine these goals by injecting uncertainty, creating potentially conflicting regulatory regimes, and increasing transaction costs with no discernible benefit to the public.

Effective immediately, all agencies and offices of **the Department that prepare regulations must ensure that any rule is not inconsistent with and does not overlap with, any regulation that has already been issued** through an agency within the Department. In the event an agency proposing that the Secretary issue a rule discovers that such rule is inconsistent or overlaps with another Department rule, the proposing agency shall not recommend issuance until it also recommends to the Secretary the steps to be taken to avoid duplicative or overlapping regulations.

Collection of information requirements: This document does not impose information collection requirements.

Brian Harrison,
Chief of Staff, Department of Health and Human Services.
[FR Doc. 2020-26023 Filed 11-24-20; 8:45 am]
BILLING CODE 4150-03-P