REQUEST FOR INFORMATION ON

CYBERSECURITY REGULATORY HARMONIZATION

AGENCY: Office of the National Cyber Director, Executive Office of the President

ACTION: Request For Information (RFI).

SUMMARY: The Office of the National Cyber Director (ONCD) invites public comments on opportunities for and obstacles to harmonizing cybersecurity regulations. Strategic Objective 1.1 of the National Cybersecurity Strategy[1] recognizes that while voluntary approaches to critical infrastructure cybersecurity have produced meaningful improvements, the lack of mandatory requirements has resulted in inadequate and inconsistent outcomes. The Strategy calls for establishing cybersecurity regulations to secure critical infrastructure where existing measures are insufficient, harmonizing and streamlining new and existing regulations, and enabling regulated entities to afford to achieve security. ONCD, in coordination with the Office of Management and Budget (OMB), has been tasked with leading the Administration's efforts on cybersecurity regulatory harmonization.[2] We will work with independent and executive branch

[1] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
[2] Pursuant to the National Cybersecurity Strategy: "ONCD, in coordination with the Office of Management and Budget (OMB), will lead the Administration's efforts on cybersecurity regulatory harmonization."

regulators to identify opportunities to harmonize baseline cybersecurity requirements for critical infrastructure.[3] ONCD seeks input from stakeholders to understand existing challenges with regulatory overlap, and explore a framework for reciprocity (the recognition or acceptance by one regulatory agency of another agency's assessment, determination, finding, or conclusion with respect to the extent of a regulated entity's compliance with certain cybersecurity requirements) in regulator acceptance of other regulators' recognition of compliance with baseline requirements.

DATE: Comments must be received in writing by **5 p.m. EDT September 15, 2023**.

ADDRESSES: Interested parties may submit comments through www.regulations.gov. For detailed instructions on submitting comments and additional information on this process, see the SUPPLEMENTARY INFORMATION section of this document.

FOR FURTHER INFORMATION CONTACT: Requests for additional information may be sent to: regharm@ncd.eop.gov.

SUPPLEMENTARY INFORMATION: In this RFI, the ONCD invites public comments on cybersecurity regulatory conflicts, inconsistencies, redundancies, challenges, and priorities, in response to the questions below. ONCD is particularly interested in regulatory harmonization as it may apply to critical infrastructure sectors and sub-sectors identified in Presidential Policy Directive 21 and the National Infrastructure Protection Plan, and providers of communications, IT, and cybersecurity services to owners and operators of critical infrastructure.

"Harmonization" as used in this RFI refers to a common set of updated baseline regulatory

[3]Pursuant to the National Cybersecurity Strategy, the Cyber Incident Reporting Council will coordinate, deconflict, and harmonize Federal incident reporting requirements. ONCD is not requesting views from respondents on incident reporting regulations.

requirements that would apply across sectors. Sector regulators could go beyond the harmonized baseline to address cybersecurity risks specific to their sectors. ONCD is also interested in newer technologies, such as cloud services, or other "Critical and Emerging Technologies" identified by the National Science and Technology Council,[4] that are being introduced into critical infrastructure.

ONCD strongly encourages academics, non-profit entities, industry associations, regulated entities and others with expertise in cybersecurity regulation, risk management, operations, compliance, and economics to respond to this RFI. We also welcome State, Local, Tribal, and Territorial (SLTT) entities to submit responses in their capacity as regulators and as critical infrastructure entities, specifying the sector(s) in which they are regulated or regulate.

Guidance for submitting comments:

- Respondents are encouraged to comment on any issues or concerns you believe are relevant or appropriate for our consideration and to submit written data, facts, and views addressing this subject, including but not limited to the questions below.
- Respondents do not need to answer all questions listed – only the question(s) for which you have relevant information. The written RFI response should address ONLY the topics for which the respondent has knowledge or expertise.
- Wherever possible, please provide credible data and specific examples to support your views. If you cite academic or other studies, they should be publicly available to be considered.

[4] https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf.

- Please provide the name of the critical infrastructure sector(s) to which you are aligned or support.
- Do not submit comment(s) in this RFI regarding harmonization of cyber incident reporting requirements. Such 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.
- All submissions are public records and may be published on www.regulations.gov. Do NOT submit sensitive, confidential, or personally identifiable information.

Questions for respondents:

1. Conflicting, mutually exclusive, or inconsistent regulations – If applicable, please provide examples of any conflicting, mutually exclusive, or inconsistent federal and 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.
b. Have these conflicting, mutually exclusive, or inconsistent rules or guidance been updated to meet new cybersecurity risks, vulnerabilities, or threats (e.g. supply chain risk)? If so, were those separate rules or guidance updated at close to the same time?

c. How do regulated entities comply with these conflicting mutually exclusive, or inconsistent requirements (e.g., follow the most demanding standard)? Please describe your experiences managing such compliance requirements.

d. For entities subject to conflicting, mutually exclusive, or inconsistent regulations, what monetary, executive or cyber defense team work hours, or other resource costs do they incur as a result of managing compliance with the different requirements that apply to them from different regulators?

e. Please identify cybersecurity requirements imposed by industry bodies, federal or SLTT agencies that you believe may be redundant.[5] Please explain in detail how the requirements in question are redundant.

f. As to the above questions, please provide the estimated annual cost over the past three years in terms of expenses or additional staff to comply with the conflicting, mutually exclusive, inconsistent, or redundant cybersecurity regulatory requirements you cite, and describe your methodology for developing those estimates.

g. Currently, how resource intensive is it for regulated entities to achieve cybersecurity compliance?

h. How often do prohibitive costs of compliance lead to meaningful security gaps?

i. How can future regulations address any prohibitive costs which lead to meaningful security gaps?

j. How can future regulations be implemented in ways which allow regulated entities to achieve security improvements at an acceptable cost?

[5] For the purpose of this RFI, "redundant" would mean that (1) the same regulated entity must comply with more than one Federal or SLTT cybersecurity requirements covering the same systems and (2) one or more of those regulations could be eliminated while the regulating agencies that issued the regulations are still able to fulfill the purpose of the regulation.

2. Use of Common Guidelines – Through the Federal Financial Institutions Examination Council (FFIEC), regulators of certain financial institutions have issued common Interagency Guidelines Establishing Information Security Standards and have developed a Common Self-Assessment Tool and an Information Security Booklet to guide examinations of entities in the financial sector.

a. Is such a model effective at providing harmonized requirements and why?
b. What challenges are associated with such a model?
c. Are there opportunities to adapt such a model to other sectors – or across multiple sectors – and if so, how?
d. Are there sectors or subsectors for which such a model would not be appropriate, and if so, why?
e. How does or could such a model apply outside the context of examination-based compliance regimes?
f. Are there opportunities to improve on such a model through common oversight approaches, and, if so, how?
g. Does your organization voluntarily apply a self-assessment tool regularly? What are good examples of helpful tools?
h. Would a common self-assessment tool improve the ability of entities to meet regulatory requirements?

3. Use of Existing Standards or Frameworks – The practice of using existing standards or frameworks in setting regulatory requirements can reduce burdens on regulated entities and help

to achieve the goals of regulatory harmonization. Under existing law[6], Federal executive agencies use voluntary consensus standards for regulatory activities unless use of such standards is inconsistent with law or otherwise impractical. In a recent report[7] from the President's National Security Telecommunications Advisory Council (NSTAC) that addressed cybersecurity regulatory harmonization, the NSTAC noted that "even though most regulations cite consensus standards as the basis for their requirements, variations in implementations across regulators often result in divergent requirements."

a. To what extent are cybersecurity requirements applicable to your industry or sector based on, consistent with, or aligned with existing standards or frameworks?

   i. Which standards or frameworks have been applied to your industry or sector?

   ii. Have these standards or frameworks been adopted in whole, either through the same requirements or incorporation by reference, or have they been modified by regulators? If modified, how were they modified by particular regulators? Has your entity or have others in your sector provided input that the regulator used to develop or adapt existing standards for your sector? If so, what are the mechanisms, frequency, and nature of the inputs?

b. Is demonstrating conformity with existing standards or frameworks that your industry is required by regulation to use readily auditable or verifiable and why?

c. What, if any, additional opportunities exist to align requirements to existing standards or frameworks and, if there are such opportunities, what are they?

[6] Public Law 104-113

[7] https://www.cisa.gov/sites/default/files/2023-04/NSTAC_Strategy_for_Increasing_Trust_Report_%282-21-23%29_508_0.pdf

4. Third-Party Frameworks – Both the government (for example, through the 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 non-governmental, 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?

5. Tiered Regulation – Different levels of risk across and within sectors may in part be addressed through a tiered model (e.g., low, moderate, or high risk)[8], potentially assisting in tailoring baseline requirements for each regulatory purpose. Tiering may also help smaller businesses meet requirements commensurate with their risk. For example, while these are not regulations, tiering into several baselines is a feature of Federal Information Processing Standard 199 and the NIST Risk Management Framework.

a. Could such a model be adapted to apply to multiple regulated sectors? If so, how would tiers be structured?

b. How could this tiered approach be defined across disparate operational environments and what might be some of the opportunities and challenges associated with doing so?

6. Oversight – Please provide examples of cybersecurity oversight by multiple regulators of the same entity, and describe whether the oversight involved IT or OT infrastructure. Some of these

[8] FIPS 199, Standards for Security Categorization of Federal Information and Information Systems (nist.gov)

questions reference a potential "regulatory reciprocity" model, under which cybersecurity oversight and enforcement as to cross-sector baseline cybersecurity requirements would be divided among regulators, with the "primary" or "principal" regulator for an entity having authority to oversee and enforce compliance with that baseline.

a. Please identify the federal, state or local agencies that are engaged in cybersecurity oversight of the same IT or OT systems, components, or data ("infrastructure") at the same regulated entity. This may be multiple federal regulatory schema, or multiple intergovernmental bodies (e.g., federal, state, local, Tribal).
b. Please describe the method(s) of cybersecurity oversight utilized by the agencies identified in your response to the question above.
c. To what extent, if any, are you aware that the agencies engaged in cybersecurity oversight of the same IT or OT infrastructure coordinate their oversight activities? Please describe.
d. Where multiple agencies are engaged in cybersecurity oversight of the same IT or OT infrastructure:
    i. Is the role of a "primary" or "principal" agency recognized? If so, please describe how.
    ii. To what extent do one or more of these agencies rely on or accept the findings, assessments or conclusions of another agency with respect to compliance with regard to certain cybersecurity requirements ("regulatory reciprocity")? Please provide specific examples.
    iii. What are the barriers to regulatory reciprocity (legal, cultural, sector-specific technical expertise, or other)?

e. Are there situations in which regulations related to physical security, safety, or other matters are intertwined with cybersecurity in such a way that baseline cybersecurity regulatory requirements from a separate Federal entity might have unintended consequences on physical security, safety, or another matter? If so, please provide specific examples.

f. If you are a regulated entity, what is the estimated annual cost over the past five years in terms of expenses or additional staff to address overlapping cybersecurity oversight of the same IT or OT infrastructure? Please describe the methodology used to develop the cost estimate.

g. Do multiple public sector agencies examine or audit your cybersecurity compliance for the same IT or OT infrastructure? If so, how many entities examine or audit the infrastructure and how often do these audits occur?

h. What, if any, obstacles or inefficiencies have commenters experienced with regard to cybersecurity oversight, examination or enforcement related to OT components, systems, or data?

i. Please provide examples of regulatory reciprocity between two or more federal agencies with respect to cybersecurity, including the recognition or acceptance by one regulatory agency of another agency's assessment, determination, finding, or conclusion with respect to the extent of a regulated entity's compliance with certain IT or OT cybersecurity requirements.

j. Are you aware of examples of regulatory reciprocity in contexts other than cybersecurity? If so, please describe briefly the agencies and the context.

k. Please provide examples of self-attestation in cybersecurity regulation. What are the strengths and weaknesses of this model?

l. Please comment on models of third-party assessments of cybersecurity compliance that may be effective at reducing burdens and harmonizing processes. For example, FedRAMP relies on Third Party Assessment Organizations (3PAOs) to perform initial assessments to inform decisions on FedRAMP eligibility. 3PAOs are accredited by an independent accreditation body.

   i. Are there circumstances under which use of third-party assessors would be most appropriate?

   ii. Are there circumstances under which use of third-party assessors would not be appropriate?

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.

b. Please provide examples of direct cybersecurity regulation of third-party service providers.

c. Please provide information regarding the costs to third-party service providers of conflicting, mutually exclusive, or inconsistent cybersecurity regulatory requirements that are passed on to them through their contracts with regulated customers. Please also provide estimated costs to a regulated customer of using a third-party service provider when conflicting, mutually exclusive, or inconsistent cybersecurity regulatory requirements are passed to the customer through contracts. In either case, please detail the methodology for developing the cost estimate.

d. Describe any two or more conflicting, mutually exclusive, or inconsistent regulation, one of which permits the use of cloud, while another does not. How does this impact your sector? Explain if these requirements also restrict the use of Managed Security Service Providers (MSSPs) and security tools that utilize the cloud.

e. Have any non-U.S. governments instituted effective models for regulating the use of cloud services by regulated entities in a harmonized and consistent manner? Please provide examples and explain why these models are effective.

f. The Department of Defense allows Defense Industrial Base sector contractors to meet security requirements for the use of the cloud by using FedRAMP-approved infrastructure. Please provide examples of how the FedRAMP process differs, positively or negatively, from other requirements. What, if anything, would need to change about the FedRAMP certification process and requirements for it to be usable to meet other cybersecurity regulatory requirements?

g. To the extent not included in response to any other question, please identify any specific Critical or Emerging Technologies that are subject to conflicting, mutually exclusive, or inconsistent regulation related to cybersecurity.

8. State, Local, Tribal, and Territorial Regulation. State, local, tribal and territorial (SLTT) entities often impose regulatory requirements that affect critical infrastructure owners and operators across state lines, as well as entities that do not neatly fall into a defined critical infrastructure sector. The New York Department of Financial Services, for example, established cybersecurity requirements for financial services companies.[9] California similarly passed a cybersecurity law requiring manufacturers of the internet-of-things (IOT) devices to take certain measures.[10] Dozens of states have followed suit to date. Companies that operate in multiple states are often required to comply with a variety of overlapping state and federal cybersecurity requirements.

a. Please provide examples where SLTT cybersecurity regulations are effectively harmonized or aligned with Federal regulations.
b. Please provide examples of regulatory reciprocity between federal and SLTT regulatory agencies.
c. Please highlight any examples or models for harmonizing regulations across multiple SLTT jurisdictions, to include Federal support for such efforts.
d. Please provide examples, if any, where regulatory requirements related to cybersecurity are conflicting, mutually exclusive or inconsistent within one jurisdiction (for example, state regulatory requirements that conflict with regulations at the local level).

9. International – Many regulated entities within the United States operate internationally. In a recent report from the President's National Security Telecommunications Advisory Council

[9] See 23 NYCRR Part 500
[10] See Senate Bill No. 327

(NSTAC), the NSTAC noted that foreign governments have been implementing regulatory regimes with "overlapping, redundant or inconsistent requirements…"

a. Identify specific instances in which U.S. Federal cybersecurity requirements conflict with foreign government cybersecurity requirements.
b. Are there specific countries or sectors that should be prioritized in considering harmonizing cybersecurity requirements internationally?
c. Which international dialogues are engaged in work on harmonizing or aligning cybersecurity requirements? Which would be the most promising venues to pursue such alignment?
d. Please identify any ongoing initiatives by international standards organizations, trade groups, or non-governmental organizations that are engaged in international cybersecurity standardization activities relevant to regulatory purposes. Describe the nature of those activities. Please identify any examples of regulatory reciprocity within a foreign country.
e. Please identify any examples of regulatory reciprocity between foreign countries or between a foreign country and the United States.

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

Comments must be received no later than 11:59pm ET 60 days from publication

By August 15, 2023, all interested respondents should submit a written RFI response, in MS Word or PDF format, with their answers to questions on which they have expertise and insights for the Government through regulations.gov.

Inputs that meet most of the following criteria will be considered most valuable:

- **Easy to review and understand:** Content that is modularly organized and presented in such a fashion that it can be readily lifted (by topic area) and shared with relevant stakeholders in an easily consumable format.
- **Expert:** The Government, through this effort, is seeking insights to understand current best practices and approaches applicable to the above topics, as well as new and emerging solutions.
- **Clearly worded/not vague:** Clear, descriptive, and concise language is appreciated. Please avoid generalities and vague statements.
- **Actionable:** Please provide enough detail so that we can understand how to apply the information you provide.
- **Cost effective & impactful**: If applicable, respondents should consider whether their suggestions have a clear return on investment that can be articulated to secure funding and support.
- **Strategic shifts**: Challenges that seem to be intractable and overwhelmingly complex can often be resolved with a change in perspective that unlocks hidden opportunities and aligns stakeholder interests. We welcome these ideas as well.

Kemba E. Walden

Acting National Cyber Director