From: doe.ocio.executive-secretariat
Sent: Monday, April 25, 2022 10:39 AM
To: CSF-SCRM-RFI <CSF-SCRM-RFI@nist.gov>
Cc: doe.ocio.executive-secretariat <doe.ocio.executive-secretariat@hq.doe.gov>
Subject: Comments regarding Request for Information about Evaluating and Improving Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Good morning,

Please find attached comments from the Department of Energy, Office of the CIO. An executive summary is also provided below.

Attached you'll find the NIST Request for Information (RFI) on Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management.

There was a list of 14 questions / topics provided by NIST that may be addressed in the submitted comments. The CRM attached above contains our responses to these questions / topics.

The S&A / Policy team completed the answers for Questions 1-4, ECRM team completed Questions 5-10, and SCRM team completed Questions 11-14.

Executive Summary:

- The National Institute of Standards and Technology (NIST) is soliciting feedback through a Request for Information (RFI) from Federal Agencies to understand any improvements and updates that can be made to its cybersecurity resources.
    - Resources can include the "Framework for Improving Critical Infrastructure Cybersecurity" (also referred to as the NIST Cybersecurity Framework (CSF)) and a variety of existing and potential standards, guidelines, and other information, including those relating to improving cybersecurity in supply chains.
- Additionally, NIST plans to launch the National Initiative for Improving Cybersecurity in Supply Chains (NIICS) to address cybersecurity risks in supply chains.
- NIST seeks updates to the CSF, as it was last updated in April 2018 and much has changed since then in the cybersecurity landscape in terms of threats, capabilities, technologies, education and workforce. The availability of resources to help organizations better manage cybersecurity risk has also transformed over the past few years.
- Responses to this RFI will inform a possible revision of the CSF as well as the NIICS initiative.
- There are several questions / topics posed to generate comments that contain suggested changes and feedback. Comments may address these questions, or any other topic believed to have implications for the improvement of the NIST CSF or NIST's

cybersecurity guidance regarding supply chains. NIST will consider all relevant comments in the development of the revised Framework and guidance regarding supply chains.

- The questions touch on the usefulness of the NIST CSF, the relationship of the NIST CSF to other risk management resources, and cybersecurity Supply Chain Risk Management.

Impact to OCIO: Any feedback submitted to NIST that modifies the CSF or supply chain guidance will have immediate and long-term impacts to OCIO, as IM-30 incorporates NIST guidance into its programmatic and strategic planning documentation. Impacts can include changes to the Risk Register process. Additionally, with the launch of NIICS, IM-30 can incorporate guidance stemming from this initiative into its SCRM program.

Summary of Recommendations: The comments provide feedback on the usefulness of the CSF to OCIO activities and challenges associated with following NIST guidance, as well as suggested improvements that can be made. Improvements include integration of the CISA ZTA Maturity Model and providing additional assessment guidance. In addition, the need for the inclusion of OT and IoT is highlighted as this is critical to many systems in the Department of Energy.

Please let us know if you have any questions!

Executive Secretariat
Office of the Chief Information Officer
U.S. Department of Energy

Item #	Source	Date	Name	Document Name	Question / Topic	Comment Classification	Comment
1	IM-30	4/20/2022	Amy Hamilton	Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management	The usefulness of the NIST Cybersecurity Framework for aiding organizations in organizing cybersecurity efforts via the five functions in the Framework and actively managing risks using those five functions.	(S) Substantive	The NIST Cybersecurity Framework (CSF) has been useful in aiding the Office of the Chief Information Officer (OCIO) in organizing the Department of Energy's (DOE) cybersecurity efforts across the five functions in the CSF. OCIO's vision is to improve IT services and strengthen DOE's cybersecurity posture, which in doing so will advance DOE's missions and services. Through implementation of the CSF by releasing DOE Order (O) 205.1C, Department of Energy Cyber Security Program, it enables leadership with the programmatic and operational flexibility necessary to make consistent, risk-informed investment decisions. DOE O 205.1C calls for a risk management approach that includes both quantitative and qualitative methods to mature risk management across the enterprise with the latest industry risk approaches that support informed cybersecurity risk decision-making.
2	IM-30	4/20/2022	Amy Hamilton	Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management	Current benefits of using the NIST Cybersecurity Framework. Are communications improved within and between organizations and entities (e.g., supply chain partners, customers, or insurers)? Does the Framework allow for better assessment of risks, more effective management of risks, and/or increase the number of potential ways to manage risks? What might be relevant metrics for improvements to cybersecurity as a result of implementation of the Framework?	(S) Substantive	Benefits of using the NIST CSF include advancement of the Department's mission through the collaborative development and adoption of enterprise-wide cybersecurity policies matched by prioritized risk management. By prioritizing risk management, risk decisions and mitigation investments are focused on enabling operations while balancing risk, resource constraints, and the need for innovation. A documented approach, guidance, and requirements facilitates the creation of designated roles and responsibilities, baseline performance measures, and benchmarks. Through performance measures and benchmarking, a cost-effective capability can be realized by leaders to support and defend choices with demonstrable value, risk reduction, and cybersecurity maturity progress. Cybersecurity threats exploit the increased complexity and connectivity of critical IT and OT infrastructure systems and assets. DOE has established the eCRM program to document a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk to the DOE's missions, operations, and assets. Having a common Cybersecurity Framework fosters collaboration across Agencies. When there is a common framework to build upon, it allows partners to share insights, success stories, and roadblocks that are more easily applied to across an organization.
3	IM-30	4/20/2022	Amy Hamilton	Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management	Challenges that may prevent organizations from using the NIST Cybersecurity Framework or using it more easily or extensively (e.g., resource considerations, information sharing restrictions, organizational factors, workforce gaps, or complexity).	(S) Substantive	Challenges that may prevent DOE from using the CSF include budget and resource constraints and workforce gaps. Additionally, the federated nature of DOE can add to this challenge. With Departmental Elements (DEs) / Sites having the autonomy to execute their own cybersecurity programs, it can be a challenge to have a centralized framework that can be interpreted and built upon uniquely per DE / Site.
4	IM-30	4/20/2022	Amy Hamilton	Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management	Any features of the NIST Cybersecurity Framework that should be changed, added, or removed. These might include additions or modifications of: Functions, Categories, or Subcategories; Tiers; Profile Templates; references to standards, frameworks, models, and guidelines; guidance on how to use the Cybersecurity Framework; or references to critical infrastructure versus the Framework's broader use.	(S) Substantive	One valuable addition to the CSF can be incorporating the CISA Zero Trust Maturity Model into the NIST Cybersecurity Framework. Aligning the NIST approach with the ZTA Pillars and Steps would provide additional guidance and common footing for maturing the capabilities and adoption associated with the CISA ZTA Maturity Model. While there are other ZTA Maturity Models that can be followed, aligning the NIST Framework to a single ZTA Maturity Model would further promote a common toolset across organizations and their partners.
5	IM-30	4/20/2022	Amy Hamilton	Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management	Impact to the usability and backward compatibility of the NIST Cybersecurity Framework if the structure of the framework such as Functions, Categories, Subcategories, etc. is modified or changed.	(S) Substantive	Changes or modifications to the structure of the NIST CSF, such as its' Functions, Categories, Subcategories can create impacts to the ECRM Risk Register process, which can furthermore alter executive-level reporting. Any modifications of these Functions and Categories will change how DOE aligns risks at the Site and Program level. Furthermore, the results of Risk Register data calls are reported at the executive-level to help support and drive risk management decisions. Executive-level reporting will need to be assessed to ensure it captures relevant changes made to the Risk Register process and maintains an organizational understanding of the cybersecurity risk landscape across systems, people, assets, data, and capabilities.
6	IM-30	4/20/2022	Amy Hamilton	Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management	Additional ways in which NIST could improve the Cybersecurity Framework, or make it more useful.	(S) Substantive	An additional way NIST can improve the Cybersecurity Framework is by integrating a maturity model and/or assessment guidance that can assist organizations in understanding their position and progress in implementation efforts. Inclusion of this information and guidance can augment the implementation tiers already included in the CSF.
7	IM-30	4/20/2022	Amy Hamilton	Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management	Suggestions for improving alignment or integration of the Cybersecurity Framework with other NIST risk management resources. As part of the response, please indicate benefits and challenges of using these resources alone or in conjunction with the Cybersecurity Framework. These resources include: • Risk management resources such as the NIST Risk Management Framework, the NIST Privacy Framework, and Integrating Cybersecurity and Enterprise Risk Management (NISTIR 8286). • Trustworthy technology resources such as the NIST Secure Software Development Framework, the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline, and the Guide to Industrial Control System Cybersecurity. • Workforce management resources such as the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity.	(S) Substantive	Benefits of using NIST SP 800-30 Guide for Conducting Risk Assessments in conjunction with the CSF is it informs ECRM Risk Register processes and provides a taxonomy and implementation guidance for categorizing and assessing risk. Risks are aligned to the CSF Functions and Categories and then assigned a risk level in accordance with NIST SP 800-30. Jointly leveraging these two documents provides visibility over identified risks.
8	IM-30	4/20/2022	Amy Hamilton	Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management	Use of non-NIST frameworks or approaches in conjunction with the NIST Cybersecurity Framework. Are there commonalities or conflicts between the NIST framework and other voluntary, consensus resources? Are there commonalities or conflicts between the NIST framework and cybersecurity-related mandates or resources from government agencies? Are there ways to improve alignment or integration of the NIST framework with other frameworks, such as international approaches like the ISO/IEC 27000-series, including ISO/IEC TS 27110?	(S) Substantive	This question is outside the scope of DOE IM-30's ECRM Program.
9	IM-30	4/20/2022	Amy Hamilton	Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management	There are numerous examples of international adaptations of the Cybersecurity Framework by other countries. The continued use of international standards for cybersecurity, with a focus on interoperability, security, usability, and resilience can promote innovation and competitiveness while enabling organizations to more easily and effectively integrate new technologies and services. Given this importance, what steps should NIST consider to ensure any update increases international use of the Cybersecurity Framework?	(S) Substantive	This question is outside the scope of DOE IM-30's ECRM Program.

10	IM-30	4/20/2022	Amy Hamilton	Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management	References that should be considered for inclusion within NIST's Online Informative References Program. This program is an effort to define standardized relationships between NIST and industry resources and elements of documents, products, and services and various NIST documents such as the NIST Cybersecurity Framework, NIST Privacy Framework, Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53), NIST Secure Software Development Framework, and the NIST Internet of Things (IoT) Cybersecurity Capabilities Baseline.	(S) Substantive	One reference that should be considered for inclusion within the NIST's Online Informative References Program is NIST SP 800-30, Guide for Conducting Risk Assessments. Risks can be aligned to the CSF Functions and Categories and assigned a risk level in accordance with NIST SP 800-30.
11	IM-30	4/20/2022	Amy Hamilton	Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management	National Initiative for Improving Cybersecurity in Supply Chains (NIICS). What are the greatest challenges related to the cybersecurity aspects of supply chain risk management that the NIICS could address? How can NIST build on its current work on supply chain security, including software security work stemming from E.O. 14028, to increase trust and assurance in technology products, devices, and services?	(S) Substantive	As a new effort by NIST to work with the private sector to improve supply chains, recommend NIICS create awareness, set expectations, and define guidance to assist suppliers in maintaining and providing cybersecurity supply chain information to Federal Agencies. This is especially true for small businesses that may not have dedicated resources and are sometimes reluctant to provide responses to Supply Chain Risk Management (SCRM) questionnaires or artifacts. Some suppliers have requested additional NDAs to be signed before completing a SCRM questionnaire and have stated that the work to complete a questionnaire will incur additional costs or will complete the questionnaire with artifacts if they know the product will be procured. Some suggestions for NIST to build on its current efforts for EO 14028 are as follows: • Identity minimum requirements and guidance suppliers that need to be met in order for their products to be eligible for procurement by Federal Agencies. For example, there may be different requirements by critical software categories or system classification (low, medium, high). • Create awareness with suppliers on required artifacts (e.g., Software Bill Of Materials) to provide to the Federal Agencies. • Identify role(s) that a supplier is accountable and responsible for to work with Federal Agencies. • Establish a federal certification process like FEDRAMP to facilitate identifying and procuring products that meet requirements. • Develop a capability to share information about relevant findings with other federal agencies. While each federal agency has different missions and therefore different risk tolerances, there should be a central place to share information on relevant findings on suppliers and their supply chain.
12	IM-30	4/20/2022	Amy Hamilton	Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management	Approaches, tools, standards, guidelines, or other resources necessary for managing cybersecurity-related risks in supply chains. NIST welcomes input on such resources in narrowly defined areas (e.g. pieces of hardware or software assurance or assured services, or specific to only one or two sectors) that may be useful to utilize more broadly; potential low risk, high reward resources that could be facilitated across diverse disciplines, sectors, or stakeholders; as well as large-scale and extremely difficult areas.	(S) Substantive	Recommend NIICS and NIST use a risk-based approach for a Supply Chain Risk Management (SCRM) program where the greater the risk, the greater the diligence conducted on the supplier to manage cybersecurity-related risks in supply chains. The SCRM program should conduct assessments on suppliers to include Cloud Service Providers (CSPs), resellers, and their products and services, as well as conducting assessments on open-source software that can be downloaded directly. The SCRM program should use validated data sources with the capability to view suppliers and their sub-tier suppliers. To bring a holistic approach to SCRM within a federal agency, recommend integrating SCRM into other functional groups, such as procurement and intelligence. For example, requiring suppliers to complete the questionnaire as part of the procurement process to improve supplier response. Also recommend positioning the SCRM program as a common controls' provider leveraging the federal agency's GRC tool. Finally, with NIICS working with the private sector, recommend NIICS consider leading commercial practices around SCRM in its guidance.
13	IM-30	4/20/2022	Amy Hamilton	Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management	Are there gaps observed in existing cybersecurity supply chain risk management guidance and resources, including how they apply to information and communications technology, operational technology, IoT, and industrial IoT? In addition, do NIST software and supply chain guidance and resources appropriately address cybersecurity challenges associated with open-source software? Are there additional approaches, tools, standards, guidelines, or other resources that NIST should consider to achieve greater assurance throughout the software supply chain, including for open-source software?	(S) Substantive	Additional approaches NIST should consider is adopting a uniform approach or mapping for the multiple technologies noted above (ICT, IoT, OT, IT) to help technology focused functional groups within an organization define more effective security requirements versus a compliance exercise. For example, IT and OT are sometimes managed through different roles, disciplines, and guidance within an organization, which can sometimes create misunderstandings between definitions and guidance on cyber controls for IT and OT systems. Additionally, current Supply Chain Risk Management (SCRM) guidance does not cover hardware / software that is procured outside of the FITARA process (e.g., ODC and direct purchase) as well as open-source software that is directly downloaded which is not covered by SSDF NIST 800-218. Open-source software that is directly obtained should be scanned to validate the version used has the required cybersecurity controls in place.
14	IM-30	4/20/2022	Amy Hamilton	Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management	Integration of Framework and Cybersecurity Supply Chain Risk Management Guidance. Whether and how cybersecurity supply chain risk management considerations might be further integrated into an updated NIST Cybersecurity Framework—or whether and how a new and separate framework focused on cybersecurity supply chain risk management might be valuable and more appropriately be developed by NIST.	(S) Substantive	Recommend integrating C-SCRM into the existing RMF in the beginning due to the multiple Supply Chain related guidance released and being updated, including NIST 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations for Supply Chain, and new Supply Chain Risk (SR) controls from NIST 800-53 Rev 5. If NIST / NIICS seeks to develop a dedicated C-SCRM framework, recommend NIST / NIICS provide specific guidance and requirements for suppliers and federal agencies on the different frameworks.