PUBLIC SUBMISSION

As of: 4/27/22 7:09 AM
Received: April 25, 2022
Status: Pending_Post
Tracking No. l2f-9q2f-b1xd
Comments Due: April 25, 2022
Submission Type: Web

Docket: NIST-2022-0001
Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

Comment On: NIST-2022-0001-0001
RFI-2022-03642

Document: NIST-2022-0001-DRAFT-0063
Comment on FR Doc # N/A

Submitter Information

Email: [redacted]
Organization: ISACA

General Comment

See attached file(s)

Attachments

NIST Cybersecurity RFI_ISACA Input_20220425_Final

Topic: NIST Cybersecurity RFI

DEPARTMENT OF COMMERCE National Institute of Standards and Technology
[Docket Number: 220210–0045]

Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

April 25, 2022

Thank you for the opportunity to submit comments on the NIST Cybersecurity Framework and Cybersecurity Supply Chain Risk Management RFI. ISACA is a non-profit professional association that has been in existence for over 50 years. On behalf of the approximately 157,000 members of ISACA worldwide, more than 50,000 of which live and work in the United States, it is an honor to also serve as the current steward of the Capability Maturity Model Integration (CMMI) Version 2.0 (V2.0) ecosystem and its current and growing customer base, many of which are using the NIST Cybersecurity Framework as a basis for their cybersecurity posture.

For 25+ years, high-performing organizations have achieved clear, sustainable business results with ISACA®'s CMMI® maturity models. Originally created for the U.S. Department of Defense to assess the quality and capability of their software contractors, ISACA's CMMI models have expanded beyond software engineering to help organizations around the world, in any industry, understand their current level of capability and performance and offer a guide to optimize business results.

Our integrated CMMI product suite provides best practices that enable organizations to improve performance of their key capabilities, providing a clear roadmap for building, improving, and benchmarking capability.

ISACA's CMMI model is a proven set of best practices organized by critical business capabilities which improve business performance. It is designed to be understandable, accessible, flexible, and integrate with other methodologies such as agile.

ISACA's CMMI Solutions include:

1. Capability Maturity Model Integration (CMMI)®
2. Medical Device Discovery Appraisal Program (MDDAP)
3. CMMI Cybermaturity Platform

While the original CMMI model and framework was originally developed by Carnegie Mellon University, ISACA has since updated the model to meet today's overall business and operations challenges for both the public sector and the industrial base it relies on commercially to deliver on the mission. The value of CMMI as a result of this modern 2.0 refresh helps organizations account for the following four areas:

1. Improve business performance against basic fundamentals of time, budget, customer satisfaction and other key drivers.
2. Build agile resiliency and scale with direct guidance on how to strengthen agile with Scrum project processes with a focus on performance.
3. Increase the value of benchmarking by providing a performance-oriented appraisal method that improves reliability and consistency of benchmarks while reducing preparation time and lifecycle costs.
4. Accelerated adoption with easily accessible online guidance and direction for improving processes around both cyber and overall business objectives being met.

ISACA believes there is a great opportunity to leverage the CMMI framework as a relevant resource to enhance the NIST Cybersecurity Framework, specifically in the area of supply chain security, by providing a globally recognized resource in use by both the public sector and the broad industrial base across both hardware and software considerations alike.

We recommend that the updated framework(s) include a methodology to measure and improve performance, in a manner built on or similar to ISACA's CMMI Performance solutions. This product set and integrated product suite provides a 80-90% solution that is already in place in the federal contractor landscape and defense industrial base, with open architecture and flexibility and best practices on a holistic, continuous improvement, continuous monitoring approach to all aspects of security, cybersecurity and supply chain which can be easily integrated with other frameworks and into the existing processes that federal government contract base already have proven infrastructure to address. CMMI-Security content and best practices were released in March 2021, and we are regularly updating content based on industry trends, best practices and feedback to keep the CMMI Model and best practices current.

- Examples of key best practices included in the CMMI might be included in the NIST framework outcomes, including: Supplier Configuration Management, covering versioning, Software Build of Materials (SBOM), and related data. Suppliers System Security Plans (SSPs), Supplier Source Selection, Supplier Agreement Management, Verification/Validation, Design/Technical Solution, Product Integration, Service Delivery, Governance, Process Assets, Implementation Infrastructure all need to be considered up-front and throughout the supply chain life cycle, including retirement
- Security objectives and their related outputs, and measures should be included in supply chain contracts, including routine and continuous monitoring and as key topics in supply chain technical and management reviews
- ISACA was pleased that our COBIT model was included as an informative reference, and that ISACA was among the early adopters of the Online Informative Reference (OLIR) program. As NIST aligns frameworks (activities that need to be performed) and workforce TKSs (tasks, knowledge, and skills to accomplish those activities), it might be helpful for NIST to identify how to align those with industry certifications. One method might be to align certification tasks and learning objectives with framework outcomes. Doing so would help demonstrate how attainment of a certification (e.g., Certified Information Security Manager (CISM), Cybersecurity Practitioner (CSX-P), see also

https://www.isaca.org/credentialing) helps to fulfill framework outcomes. Doing so would support a scalable workforce to implement the requirements from frameworks such as the NIST Cybersecurity Framework and Cybersecurity Supply Chain Risk Management.

- Based on other frameworks and best practices, there are several key points that NIST should include in the Cybersecurity Framework and Cybersecurity Supply Chain Risk Management:
  - Need for holistic, integrated performance/outcomes-based approach – cannot be a "bolt on" approach, but must be integrated with existing people, processes and technologies; Supply chain cybersecurity must be treated as part of the prime/providing organization's processes, flow-down of requirements, training, and technology, not separate from the work, but a key integral part of the work, including how the suppliers outputs are integrated or interface with the prime's deliverables and products
- We recommend that NIST remind those implementing frameworks to avoid a compliance-based only approach. A compliance-only focus typically assumes that quality/performance is a guaranteed outcome – this is typically NOT true. A compliance-based approach is typically inflexible and puts long-term change, innovation, and improvement at risk. Compliance also tends to become additional level of administrative overhead without clear value to performance – supply chain cybersecurity in this case, or the bottom line. Innovation and performance improvement for supply chain cybersecurity and risk requires discipline. Each aspect must be counterbalanced by tougher behavior that's less fun…rigorous discipline, a high level of individual accountability, and strong leadership[1]. NIST should continue recent work to supply quick start guides, implementation guidance, and learning videos that highlight the benefit of a holistic approach (and diminish efforts to chase conformance as the end goal.)

Thank you for your consideration. Our team of experts and academics would be pleased to work with you in resolving the questions you must reconcile. We can be reached by contacting Ron Lear with ISACA at [redacted]

[1] *The Hard Truth About Innovative Cultures*, Pisano, Gary, Harvard Business Review, Issue 97, Jan/Feb, 2019