Department of Commerce

National Institute of Standards and Technology

Recommendations for the Cybersecurity Framework

Request for Information Response

Submitted On: April 25, 2022

Submitted To:
Department of Commerce
National Institute of Standards and Technology
POC: Katherine MacFarland
CSF-SCRM-RFI@nist.gov
100 Bureau Drive, Stop 2000,
Gaithersburg, MD 20899
USA

Submitted By:
CGI Federal Inc.
12601 Fair Lakes Circle
Fairfax, Virginia 22033
703-227-6000
www.cgi.com

TABLE OF CONTENTS

1. OVERARCHING FRAMEWORK

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) rightfully holds a place as the national, and arguably global, conceptual standard upon which cybersecurity programs are built. It establishes commonality in terminology and approach, and the five functions are conceptually delineated in a way that just about any security program can be aligned within them, if taken at the right level of abstraction.

Case in point, our modern approach to delivering security operations builds alignment between two different, but relatable frameworks in the concept of a centralized security operations center (SOC) that treats all threats in accordance with the framework, internal and external alike. We align the two frameworks leveraging the CSF and the core framework model. This makes it easier for us to build technical solutions and business processes that reliably mitigate threats, manage and automate incident response, recover, and feed lessons learned back into continuous improvement programs.

As we view the CSF as an extensible framework in this manner, one that allows any security continuum to map to "Identify, Protect, Detect, Respond, and Recover", we recommend that no substantive structural changes to the framework be made at the top level of abstraction.

2. SUPPLY CHAIN RISK MANAGEMENT INTEGRATION

Our ongoing work to more seamlessly integrate NIST's published Information and Communications (ICT) Supply Chain Risk Management (SCRM) guidance into our approach for customer solutions includes mapping the SCRM program in a fashion similar to that stated above. This approach builds out our concept of a "Supply Chain Security Operations Center", which operates in concert with the Cyber SOC and increases operational efficiencies through symmetric security and incident response processes. The following recommendations are derived from challenges or inefficiencies we have observed in making that integration.

2.1 Supply Chain Risk Management (SCRM) High-Level Alignment with the CSF

The NIST Special Publication (SP) 800-161, *"Supply Chain Risk Management Practices for Federal Information Systems and Organizations"* framework is built on four functions: "Frame, Assess, Respond and Monitor", as **Figure 1** represents. We have found that effort is required to align the frameworks, and while this is not an insurmountable task, it does require the development of a translation document which must be maintained and updated by us or our customers.

As such, we recommend consideration be given to refactoring NIST 800-161's approach to more explicitly map to the five CSF functions. We believe this will increase the ease of adoption across industry, and deliver more successful implementations of cohesive and integrated security programs.

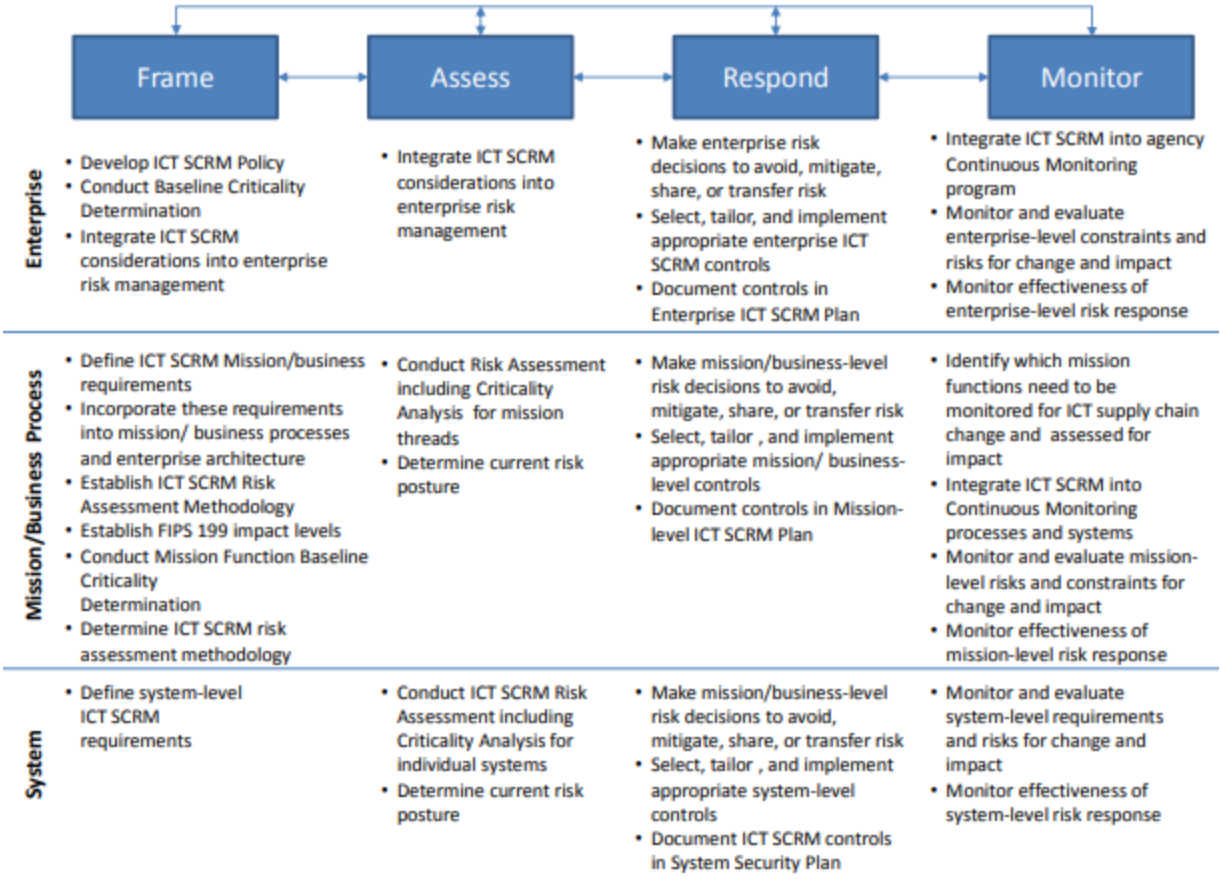

Figure 1: ICT SCRM Framework from Figure 2-4 of NIST SP 800-161

2.2 Improve Alignment of SCRM Categories within the CSF

The CSF Core specifically addresses SCRM within the "Identify" function as the category Supply Chain Risk Management (ID.SC), with subcategories ID.SC-1 through ID.SC-5. Some of these subcategories, however, appear to be more appropriately mapped to other functions within the CSF Core, or otherwise worthy of amplification within the text of the Core.

2.2.1 ID.SC-3

ID.SC-3 states: *"Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan."* There is a component here that is appropriate for the "Identify" function, in that the implementer should identify the appropriate contractual requirements to invoke upon suppliers. These requirements may include appropriate evidence and/or attestations of secure software development practices; requirements for notifications regarding foreign, ownership, control, or influence (FOCI) changes; software bill of materials (SBOMs), and; vulnerability disclosure program (VDP) participation as appropriate.

These requirements, however, do not have a corresponding subcategory in the "Detect" function, and the operationalization of these contract requirements should be reflected in other areas within the framework, similar to other cyber operations. As an example, integrating SBOMs into

vulnerability management programs and consuming vulnerability exchange (VEX) data to detect for issues, or monitoring upstream suppliers for risk indicators such as breaches, financial stress, FOCI changes, etc., would be appropriate for reference in the "Detect" function as dedicated subcategories akin to continuous monitoring. Further, as any anomalies triggered by supply chain oversight should be formally responded to, adding an appropriate subcategory to the "Respond" function would be useful.

Additionally, in the "Informative References" table for ID.SC-3, a direct reference to NIST SP 800-161 might be beneficial.

2.2.2 ID.SC-4

ID.SC-4 states: *"Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations."* Similar to the rationale above, this appears to be an operational action that is better suited to the "Detect" function within the framework.

2.2.3 ID.SC-5

ID.SC-5 states: *"Response and recovery planning and testing are conducted with suppliers and third-party providers."* This critical function parallels that in the Information Protection Processes and Procedures (PR.IP) subcategory 10 (PR.IP-10), which states that *"Response and recovery plans are tested."* Similarly, it would be appropriate for ID.SC-5 to be merged with (by explicit expansion) PR.IP-10, or given its own place within the "Protect" function for exercising such plans.

2.2.4 Communicating Cybersecurity Requirements with Stakeholders (Section 3.3)

While the CSF publication itself is not intended to be a completely stand alone or all-inclusive compendium of information, it does provide some introductory discussion on communicating cybersecurity requirements with stakeholders, including those pertaining to SCRM. This is useful, and as such, consideration should be given to incorporating some additional discussion on some of the relevant fundamental elements of the Secure Software Development Framework (SSDF) and other pertinent definitions and references for "Critical Software", SBOM, and Supplier Declaration of Conformance, as they have clear and distinct impact to supply chain requirements, as well as overall cybersecurity.

2.2.5 Workforce Framework for Cybersecurity

We have been successful in leveraging the National Initiative for Cybersecurity Careers and Studies™ Workforce Framework for Cybersecurity (NICE Framework) for building models of cybersecurity organization implementations. The NICE Framework, as we use it, requires extension in order to align Insider Threat SOC functions with the Cyber SOC functions. We see similar need for extension pertaining to the integration of SCRM within a SOC construct. The Securely Provision – Risk Management section of the framework should include roles, tasks, and knowledge-skills-abilities (KSAs) for SCRM analysts, as well. This extension will aid in aligning and utilizing the NICE Framework with the CSF, as they are quite complimentary.

3. IMPROVING IMPLEMENTATION THROUGH PLAYBOOKS

The Cybersecurity Framework extensively references NIST SP 800-53 rev 4 with regard to supply chain integrity controls and standards. The NIST SP 800-161 also has an extensive set of controls and processes for implementation of supply chain security, and ensuring supply chain integrity.

NIST SP 800-161 also references NIST SP 800-53 rev 4 throughout causing some confusing loops when trying to plot a course for supply chain integrity approaches. This is one example of a pattern recognized across multiple special publications produced by NIST.

To interpret, implement, document, and validate the framework, a business is required to employ numerous resources with specific, and often non-overlapping, skills and domain expertise. The alternative practice of hiring consulting firms creates a difficult barrier of entry to overcome for most small businesses. While these realities do help to ensure that cybersecurity is properly addressed in government systems, they can often prevent innovative and effective solutions from making it to market.

Our suggestion is to develop a set of targeted playbooks that provide more specific approaches based on qualifying factors. A simple example would be to target a general industry, such as software development, and provide guiding examples to implement cybersecurity controls into the application lifecycle. Information Technology consultants could use a playbook targeting common systems they support, such as domain management and email hosting solutions. All of these playbooks should follow best practices, such as zero trust architecture. These playbooks could reduce time to entry by giving technologists the ability to implement with security "baked in."