Deloitte & Touche LLP
1919 North Lynn Street
Arlington, VA 22209

Tel: +1 (571) 882-5000
www.deloitte.com

April 25, 2022

National Institute of Standards and Technology (NIST)
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899
Submitted electronically to CSF-SCRM-RFI@nist.gov on April 25, 2022

RE: **Deloitte & Touche LLP Comments on "Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management"**

To Whom It May Concern,

Deloitte[1] appreciates this opportunity to submit comments in response to NIST's Request for Information (RFI) for evaluating and improving the Cybersecurity Framework (CSF) and Supply Chain Risk Management. As one of the largest professional services organizations in the United States, Deloitte provides a vast array of information security services across 2,800 engagements in major commercial industries and 15 cabinet-level federal agencies. We serve our clients by helping them align their security and privacy investments with business risk priorities. Our comments reflect our deep history with the NIST CSF—having originally supported NIST in its development—as well as our implementation experience with customers who are applying the CSF, other standards and guidelines, and supply chain risk management processes across their businesses and government departments.

Again, we appreciate the opportunity to comment on the "Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management" RFI and highly value the open engagement that NIST continues to foster on critical cybersecurity topics. In the event that the provided comments will be circulated outside the NIST review group, we ask that Deloitte be notified prior to distributing materials. Should you have questions regarding our comments, please contact us.

[1] As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

Respectfully submitted,

Sharon Chand, Principal

Colin Soutar, Managing Director

Government and Public Services | Risk & Financial Advisory
Deloitte & Touche LLP

Use or disclosure of the data contained on this page is subject to the restrictions on the title page of this request.
Copyright © 2022 Deloitte Development LLC. All rights reserved.

Contents

Introduction

Deloitte applauds NIST's efforts to evaluate and improve its existing cybersecurity resources, including the NIST Cybersecurity Framework (CSF) and the National Initiative for Improving Cybersecurity in Supply Chains (NIICS). We believe that using the CSF and other NIST frameworks and guidelines to support technology developers, providers, and acquisitions specialists is an effective approach for cyber risk management, and we look forward to contributing to further development of these resources.

We believe the CSF could benefit from continued enhancements such as the inclusion of additional examples, templates, informative references, and updated guidance language. While the feedback we have provided on the CSF is general in nature, it is based on our years of experience helping to develop the CSF and subsequently deploying it across commercial, state and local, and federal clients. We offer more specific comments regarding Cybersecurity Supply Chain Risk Management given the emerging nature of this topic.

1. General Feedback on the Use of the NIST Cybersecurity Framework

Since the inception of the CSF, we have seen many organizations, from federal government agencies to the commercial sector, adopt CSF components to help them understand and assess their cybersecurity risk. Deloitte feels that one of the primary drivers of the CSF's success is its descriptive, rather than prescriptive, language. Organizations can tailor the CSF to fit their programs, large or small, instead of struggling to adapt to one rigid way of approaching risk. It is flexible and adaptable, but has also provided a common taxonomy that enables more consistent communication of cyber risk across and between entities. In general, Deloitte has found the CSF to work well with other NIST guidance and we support NIST's efforts to consolidate useful reference documents through the NIST Online Informative References Program. Nonetheless, there are areas for development Deloitte suggests for consideration to enhance the existing CSF. Our general feedback and comments are as follows:

Benchmarking. Today, there is a lack of insight for organizations on maturity within their respective industry and, as a result, where their organization stands in relation to others. Collaboration could be increased by facilitating an annual information sharing forum wherein organizations could present on their progress. In addition to an annual forum, NIST could consolidate and expand upon its "Success Stories" and "Perspectives on the Framework" pages for organizations to report on progress, successes, pain points, and other salient information. Discussions can be broken out by industry to enable real-time information gathering by NIST to support ongoing benchmarking. Benchmarking could be published on an annual basis, by industry. Areas where organizations are having success can be available as resources or leading practices, and pain points can serve to inform more focused forums on ways to overcome these issues. Such an information portal could help NIST better understand how organizations are using CSF. This could lend itself to an interconnected ecosystem of organizations within a certain industry, enhancing collaboration, having these organizations

Use or disclosure of the data contained on this page is subject to the restrictions on the title page of this request.
Copyright © 2022 Deloitte Development LLC. All rights reserved.

serve as a feedback loop, as well as a mechanism to gather ongoing feedback on improvement areas.

Privacy. Given that NIST 800-53 SP Rev 5 has consolidated security and privacy controls for information systems, we believe organizations can benefit from further guidance on how to use CSF in conjunction with the NIST Privacy Risk Management Framework (PRMF) to collectively address privacy and security risks. Providing guidance on creation of integrated current and target profiles and action plans utilizing both Frameworks, as well as integrated informative references in addition to existing CSF to PRMF crosswalks, can facilitate a broad approach to helping organizations reduce risks—whether privacy or security—to their operations and assets, which remains a challenge for many.

Commercial Sector. On the commercial side, Deloitte has found some clients have found the language around conducting capability assessments to be too subjective and experienced difficulties interpreting the intention behind NIST's language for Tiers. Deloitte suggests mapping some of the Tiers language to Capability Maturity Model Integration (CMMI)—as well as other commonly used organizational maturity models—and providing additional examples, use cases, and guidance to help integrate these concepts.

Outcome Specificity. For some CSF Functions, such as *Detect* and *Respond*, we are hearing that additional specificity on the Subcategory outcome language would help organizations understand gaps in their Security Operations Centers (SOC). This is particularly true with sectors such as State and Local, and there may be an opportunity for NIST to strengthen collaboration with Information Sharing and Analysis Centers (ISACs). This effort could also be furthered through standardized templates and tools to enable communities to better build their CSF profiles with more specific outcomes tailored to their own risk environments and regulatory considerations.

Use or disclosure of the data contained on this page is subject to the restrictions on the title page of this request.
Copyright © 2022 Deloitte Development LLC. All rights reserved.

2. Cybersecurity Supply Chain Risk Management

Challenges of C-SCRM

Among the primary challenges of C-SCRM today are provenance challenges with respect to builds of software products. Executive Order 14028 states the private sector must be adaptive and ensure its products are built and operated securely in a continuously changing threat environment[2]. Provenance from a software perspective has to do with tracking how the software is built and recording all the relevant metadata associated to it. Some requirements have been articulated elsewhere and are relevant to characterize these challenges in more detail.

Requirements have been articulated as the following: "(a) Providing artifacts that describe how suppliers and vendors are conforming to software security processes, (b) Provenance of software code that would allow attestation of integrity and verifiability of software code development and build processes. (c) Continuous update of software processes to compute metrics that would allow evaluation of trustworthiness of vendors and suppliers[3]." NIST can emphasize the importance of provenance capabilities to be integrated within the NIST CSF wherever possible.

A fundamental challenge of software supply chain (SCC) security pertains to how customers of software providers contract and license the use of software. Most licensing agreements contain language such as: "Licensee will not […] create or attempt to create, or permit others to create or attempt to create, by disassembling, reverse engineering or otherwise, the source program or any part thereof from the object program or other information made available to Licensee pursuant to this Agreement." While this type of restriction helps protect the software developers' intellectual property, it prevents customers and users from being able to perform deeper analysis of the software's underlying code. While software provenance and Software Bill-of-Materials (SBOMs) are useful and shed light on software origination; they ultimately do not get at the heart of malicious code, in other words what does the code itself do that could adversely impact the systems on which it is installed.

NIST has an opportunity to continue to provide more examples to the technology community that demonstrate at-scale functional models that follow the software secure supply chain guidance that has been developed—identifying practical examples where guidance is being deployed at scale.

Approaches, Tools, Standards, Guidelines, and Other Resources for Managing Cybersecurity-Related Risks in Supply Chains

Managing cybersecurity-related risks in supply chains needs to be done at scale, leveraging automation to efficiently identify areas of risk that may take additional action.

Employment of frameworks such as The Update Framework (TUF)[4] and in-toto[5], in a manner that cannot be tampered with, are approaches that NIST may consider incorporating. The ability

[2] Executive Order 14028: Executive Order on Improving the Nation's Cybersecurity, Section 1. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[3] S. Shetty and A. Rahman. (2021). Response to EO 14028 on Enhancing Software Supply Chain Security: Responses to Call for Position Papers on Standards and Guidelines. Retrieved from: https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/enhancing-software-supply-chain-security

[4] The Update Framework (TUF). (2022) Retrieved from: https://theupdateframework.io.

[5] In-Toto Framework. (2022). Retrieved from: https://in-toto.io.

Use or disclosure of the data contained on this page is subject to the restrictions on the title page of this request.
Copyright © 2022 Deloitte Development LLC. All rights reserved.

to capture relevant artifacts and associated metadata in an immutable record akin to an accessible well-performing blockchain[6] provides suggestions for such an approach. The ability to scale in alignment to cloud native principles is critical to ensure proper performance based on need[7].

A key objective is to build a system that can support security SSCs in support of durable and robust software. SSCs involve compiling, integrating, and testing software from external sources into a completed software product. In most cases, SSCs consist of a set of integrated (i.e., chained together) steps with different purposes. In some cases, these steps serve to verify; in other cases, they serve to compile. Both steps facilitate driving a software build toward a completed state where the final outcome is a usable software product. SSC security is vital to enterprise software builds and aims to thwart adversaries with the ability to influence or control SSC build steps through injecting malware at backdoors and/or vulnerabilities. Due to the multiple-step nature of building software via SSCs, attackers use breaches as a quick way to impact many users simultaneously.

Frameworks such as TUF can support developers with the ability to protect systems against repository compromises and attack vectors that focus on signing keys. TUF is a way to issue trust information about software along with providing other metainformation about these artifacts. A core goal is to authenticate the originating provider of the data stored within the repository. In addition, TUF can validate the freshness of the artifacts along with repository consistency as these are critical steps toward overall integrity and security for the software supply chain. A key objective in the application of TUF is to prevent nefarious behavior that may emanate from attackers that can mix and match software artifacts in such a way that the sum of their parts is malicious.

Frameworks such as in-toto can secure the way in which software is developed, built, tested, and packaged (e.g., SSC). in-toto attests to the integrity and verifiability of every action performed: writing code, compiling, testing, and deploying. The framework is transparent to the user regarding the steps performed (order and user). The framework enables users to perform a series of verification steps in the supply chain to determine attribution, integrity, and attestation of the transaction.

TUF and in-toto are just two examples of existing, open-source frameworks that NIST could assess and consider for integration as an informative reference in the CSF. Thorough and periodic inventories of supply chain specific risk frameworks could help the CSF integrate leading practices and maintain pace with industry changes.

Gaps in Existing Cybersecurity Supply Chain Risk Management Guidance and Resources

The provenance requirements previously articulated also directly map to current gaps that are presently challenges.

These gaps can be stated as follows:

1. An inability to document, trace, audit, or record the artifacts that describe how suppliers and vendors are conforming to software security processes;
2. An inability to document, trace, audit, or record attestation for the purposes of integrity and verifiability in all build processes; and

[6] E. Bandara, S Shetty, A Rahman, R Mukkamala. (2021) Let's Trace — Blockchain, Federated Learning and TUF/In-ToTo Enabled Cyber Supply Chain Provenance Platform. MILCOM 2021-2021 IEEE Military Communications Conference (MILCOM), 470-476. Retrieved from: https://ieeexplore.ieee.org/abstract/document/9653024.

[7] Cloud Native Computing Foundation (CNCF). (2022). Retrieved from: https://www.cncf.io/.

Use or disclosure of the data contained on this page is subject to the restrictions on the title page of this request.
Copyright © 2022 Deloitte Development LLC. All rights reserved.

3. An inability to record, document, trace, or audit the metrics that allow evaluation of trustworthiness of vendors and suppliers software code.

Open-source code provides an opportunity, since the underlying code itself is available, to perform more in-depth analysis. For example, queries can be performed to search for lines of code which tamper with system shutdown, elevate privileges, and in general, execute activities that would not be expected of the code. This type of analysis can increase user ability to trust that malicious code does not exist in the open-source code components.

Integration of CSF and Cybersecurity Supply Chain Risk Management Guidance

Consideration for updates to the current NIST CSF should be aligned around the areas that discuss Supply Chain Risk Management captured in ID.SC items (1) to (5). Each of these five items provides guidance on "Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks[8]." As previously stated, we believe that the last sentence does not capture enough "scope" to adequately provide details to help organizations address supply chain challenges. The ability to capture the artifacts and metadata associated with these processes, along with a storage system (ideally an immutable one), is important to ensure that it is tamper proof. ID.SC-4 should be considered as a particular area for modification. Including artifact data and inclusive metadata could improve this area as previously outlined.

[8] NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, pp. 28-29, National Institute of Standards and Technology. Retrieved from: https://www.nist.gov/cyberframework/framework.

Use or disclosure of the data contained on this page is subject to the restrictions on the title page of this request.
Copyright © 2022 Deloitte Development LLC. All rights reserved.