PUBLIC SUBMISSION

As of: 4/27/22 7:04 AM
Received: April 25, 2022
Status: Pending_Post
Tracking No. l2f-56uf-dn2p
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-0060
Comment on FR Doc # N/A

Submitter Information

Email: [redacted]
Organization: Fortress Information Security

General Comment

NIST Cybersecurity RFI comments are being provided by Fortress.

Attachments

NIST Cybersecurity Framework_Fortress_042522

UNITED STATES OF AMERICA
BEFORE THE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Request for Public Comments on the The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management	**)**
docket number 220210-0045	**)**

VIA Post:

Federal eRulemaking
Portal: *https://www.regulations.gov*

COMMENTS OF FORTRESS INFORMATION SECURITY AND ITS SUBSIDIARY CYBER RISK UTILITY, LLC D/B/A ASSET TO VENDOR NETWORK ("A2V")

Fortress Information Security ("Fortress") [1] appreciates the opportunity to comment on the NIST Cybersecurity Framework and Cyberscurity Supply Chain Initiative. The Framework has been of foundational importance to Fortress in developing targeted, cost-effective supply chain risk management products and services to support industry and the federal government. In providing assistance, Fortress has gained significant perspectives on the challenges that remain for securing critical supply chains, and how, in collaboration with Fortress and other industry partners, the updated Framework and National Initiative for Improving Cybersecurity in Supply Chains (NIICS) can help meet these challenges.

[1] https://fortressinfosec.com/

1. Our Background

Fortress Information Security, together with its subsidiary, Cyber Risk Utility, LLC (d/b/a the "Asset to Vendor Network or "A2V"), provides cyber supply chain risk management (C-SCRM) solutions. Our mission is to secure critical infrastructure in the energy sector and beyond by helping vendors and asset owners manage the intensifying threats to their supply chains. Fortress also helps the Department of Defense and the Department of Homeland Security secure their supply chains against especially significant nation-state threats.

Fortress delivers four capabilities for the purpose of enabling C-SCRM program execution and maturity:

1. proprietary software known as the Fortress Platform

2. an information sharing exchange known as A2V

3. vendor and product risk mangement tools, data, and analytics such as the Related Entity Discovery methodology ("RED") and File Integrity Application ("FIA"), and

4. a variety of managed services to help our clients make better risk-informed procurement decisions.

The A2V information sharing network is the only central repository in existence that correlates dozens of data sources within specific industry and government domains. A cadre of specialized research analysts and engineers conduct ongoing, comprehensive controls assessments and monitoring analyses to support data-driven solutions that address cybersecurity, Foreign Ownership Control and Influence (FOCI), component obsolescence and dependencies, and other critical risks.

2. Our Credentialed Expertise

The A2V network was created in partnership with American Electric Power ("AEP") and Southern Company ("Southern"). The A2V network is further enhanced through emerging collaborations with the US Armed Services through engagements with the Air Force and Navy. With enhanced focus on driving vendor collaboration and addressing the threats that vendors face, the A2V network is expanding with critical manufacturing OEM and system integrator partnerships. Patterned after the financial industry's success driving maturity and reducing compliance costs, the A2V information-sharing network is the only central repository focused exclusively on the unique needs of customers and their critical suppliers in the industries we serve.

As will be more fully described in our comments section, we operationalize our clients' C-SCRM programs using recognized frameworks, with a special emphasis on leveraging the National Institute of Standards and Technology ("NIST") Framework for Improving Critical Infrastructure Cybersecurity.

In assessing our clients (both asset owners and their critical suppliers), Fortress sees different maturity levels in C-SCRM programs. The A2V network drives maturity by fortifying expertise while accommodating financial constraints on less-resourced asset owners and suppliers. Instead of each organization completing its own C-SCRM assessments, Fortress conducts the risk assessments, simplifying what otherwise would be a redundant, costly, and burdensome process for asset owners and their suppliers. The A2V network increases cyber supply chain maturity by sharing information, driving best practices, and reducing compliance costs to all those involved, from asset owners and suppliers to other stakeholders such as state, local, tribal, and territorial (SLTT) governments.

We accelerate achieving C-SCRM program maturity by removing duplicative, inefficient work on behalf of every industry participant involved. The Fortress A2V central repository contains information on 40,000 vendors and products. We monitor vendors' and products' security controls, vulnerabilities, FOCI, and breaches. We have completed tens of thousands of assessments of vendors and products just in the last year. These assessments include validated vendor-control assessments, any-source vendor and product assessments, product in-depth assessments, software-Bill-of-Materials ("SBOM") assessments and hardware-Bill-of-Materials ("HBOM") assessments, geo-political relationship assessments, and Software/File Integrity Assessments ("FIA").

The highly automated, continuously updated supply chain data repository maintained by Fortress enables us to respond to the rapidly evolving needs of asset owners. For example, as Russia launched its invasion of Ukraine in February 2022, Fortress was able to assist asset owners in scrutinizing their critical supply chains for products produced by Russian and Russian-affiliated entities. The need for such rapid data analyses and sharing capabilities will grow as the security challenges posed by Russia, China, and other potential geopolitical adversaries continue to evolve.

Our work has taught us that, while asset owners and their suppliers have expended tremendous effort and resources to implement C-SCRM programs, they remain dangerously vulnerable at the C-SCRM level. The first step to a long-term, successful C-SCRM program requires growing a program's maturity and sufficient resources to support it. The threat is upon us. Time is of the essence. Collaboration and support between the private sector, government at all levels, and the cybersecurity industry is essential in achieving a successful, fully mature level of cybersecurity.

3. Our Comments

Response to Section 1. Use of the NIST Cybersecurity Framework

Fortress uses the NIST Cyber Security Framework (CSF) to help determine a baseline for supplier security controls and to help us convey to asset owners how well a supplier meets the practices described in the CSF. In terms of a standard, the CSF and North American Transmission Forum (NATF) Supply Chain Criteria/Questionnaire[2] are effective documents that help convey industry or security best practices. However, in recommending supply chain risk management industry practices, the CSF overlooks more recent and pertinent considerations. Consider the following:

- Software hygiene and malware clean-bill-of-health, which includes:
    i. Software Component Analysis (Software Bill of Materials)
    ii. Hardware Component Analysis (Hardware Bill of Materials)
    iii. Hardware or Software Geopolitical Affiliations Mapping
    iv. Third-party solutions vulnerability analysis

Response to Section 2. Relationship of the NIST Cybersecurity Framework to Other Risk Management Resources

Within the last two years, businesses globally have encountered an unprecedented number of cybersecurity compromises which, as a consequence, have placed American critical

[2] North American Transmisison Forum, *Supply Chain Cyber Security Industry Coordination*, https://www.natf.net/industry-initiatives/supply-chain-industry-coordination

infrastructure businesses on notice:

- SolarWinds: Thousands of companies were exposed by a software supply chain attack which could allow foreign adversaries back-door access into critical infrastructure
- Colonial Pipeline: A ransomware attack that caused a shutdown of oil and gas operation in southeastern region of the US
- JBS Foods: Plants were forced to shut down due to a ransomware attack which impacted nearly a quarter of all beef production in the US
- Kaseya: A software supply chain attack targeting managed service providers that exposed hundreds of businesses to unauthorized access and exfiltration of sensitive information
- Invenergy: A ransomware exploit directed at a non-grid related system, executed by the same threat organization that targeted Kaseya and Colonial
- Log4j: A newly discovered Java-based cybersecurity flaw affecting vast swaths of the Internet from Google and Amazon to the systems used to run militaries and hospitals, deemed by US Homeland Security as the most serious vulnerability seen in decades.

The takeaway from these attacks is clear. There still is no effective, centralized critical infrastructure policy that ensures the required cybersecurity hygiene, information sharing, and supply chain security that would enable asset owners and operators to quickly react to cybersecurity, supply chain and ransomware attacks. No one doubts the need for increased government scrutiny of cybersecurity. The more important question is how to maximize existing regulations, best practices, and standards to ensure that the next policy direction is effective.

Purchasers of Information Communication Technologies (ICT) for critical applications and technologies reqiure assurances that the products they intend to implement constitute an effective C-SCRM solution. Assurances can be in the form of a central repository of attestations, conformance to industry standards that can be audited for compliance, and independent validation or certification. Third-party validation or certification is effective at assuring the purchaser that specific controls and standards are being met, or that the supplied technologies conform to recognized standards, such as ISA/IEC 62443-4-1for secure development practices. In addition, defining the relationship of NIST 161[3] to the CSF 2.0 would serve to highlight supply chain best practices. Importantly, there currently are no consensus-based standards that fully address security concerns associated with FOCI (Foreign Ownership Control or Influence), SBOM or HBOM risks. An effective ICT product security standard should address application or system development practices, geopolitical risks, and component transparency as part of addressing supply chain best practices.

From a policy standpoint, EO 14017 is sound and appropriate, given US critical infrastructure and reliance on foreign-manufactured ICT. Because of reliance on third-party-designed, developed, and maintained technologies, additional emphasis should be placed on the origins of manufacturing. The administration should require that high-risk ICT acquisitions undergo C-SCRM vetting. There are several emerging laws and regulations that appear to be directionally supportive of securing ICT and critical infrastructure supply chains. The first of these is the proposed DHS Software Supply Chain Risk Management Act of 2021 (H.R. 4611) bill. It recognizes the need for product transparency using bills of materials. Software or hardware bills of materials are crucial for providing key information about the components

[3] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

within applications and devices procured from vendors and suppliers. This type of legislation would be invaluable in supporting and mitigating ICT supply chain risks. The proposed Cyber Sense Act of 2021, while focused on the bulk bulk electric system, could be an excellent means to ensure that technologies used on the electric grid are tested to determine if vulnerabilities exist and how they can be mitigated to ensure the reliable operation of the power grid. Executive Order 14028 outlines several initiatives for NIST (National Institute of Standards and Technology) to develop standards for citical software, software supply chain security and cybersecurity labeling. Each of these initiatives, facilitated through the EO 14028, can support the security and protection of America's supply chains.

Other considerations regarding supply chain security standards include the following:

- FEDRAMP Gov, SOC 2 or the equivalent, for cloud, or at the service-function controls level
- ISO 27001, NIST SP 800-53 or the equivalent, for information security controls
- ISA/IEC 62443 or the equivalent, for SDL practices and product security controls

Response to Section 3. Cybersecurity Supply Chain Risk Management

Asset owners must currently rely on a relatively limited number of reputable suppliers for critical hardware products. For vital SCADA (Supervisory Control and Data Acquisition) systems, even fewer such suppliers are avaible. Moreover, as in the case of battery technologies for electric vehicles and energy storage, as well as the inverters essential for expanding solar and wind power production, asset owners have few options for procurement from companes in the US or allied nations. As NIST goes forward with the National Initiative for Improving Cybersecurity in Supply Chains (NIICS), consideration should be given to incentivizing or

otherwise increasing the availability of domestic and ally-produced products. However, as with any such changes in markets and manufacturing, it takes time for quality competitors to emerge to help ensure availability of numerous sourcing options to reduce the risk of single points of failure or common-mode failures. In addition, purchasers may not be aware of alternative technology or service providers that may meet their procurement requirements. Supply chain risk management solutions, such as Fortress A2V, can help identify, categorize, and maintain updated lists of qualified suppliers who can provide purchasers with recognized alternatives.

In unpdating the NIST Framework and launching the NIICS initiative, NIST might also consider the following recommendations derived from our extensive experience in helping our clients neutralize supply chain threats:

1. Establishing Risk-Based Critieria for Gathering and Analyzing Data for Supply Chain Risk Management

Executive Order (EO) 14028, Improving the Nation's Cybersecurity, released on May 21, 2021, called attention to the value of focusing software supply chain security initiatives on those software components that perform notably critical functions.[4] In alignment with the supply chain standards established for the Bulk Electric System by the North American Electric Relaibility Corporation (NERC), Fortress has developed a risk-based approach to help clients prioritize their supply chain management programs. NIST would be well-advised to consider establishing equivalent risk criteria (factoring in supply chain threats, vulnerabilities, and consequences of a

[4] Executive Order 14028, *Improving the Nation's Cybersecurity*, May 21, 2021, pp. 1 and 7, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

successful supply chain penetration/exploitation) for adoption across multiple infrastructure sectors.

2. Continuous, Automated Updating of Risk Data

As noted above, owing to its highly automated data repository and access systems, Fortress was able to rapidly respond to asset-owner requests for data on potential supply chain threats from Russia. The National Telecommunications and Information Administration (NTIA) has found that the key "for SBOM to scale across the software ecosystem, particularly across organizational boundaries, is support for automation, including automatic generation and machine-readability."[5] Requirements for automation will be more extensive to manage risks of supply chain threats from China, Russia, and other nations capable of highly sophisticated attacks. As grid vendors and their partners strengthen their defenses, foreign adversaries will be sure to seek out new supply chain vulnerabilities (including clandestine, infiltrated subcontractors) to exploit and leverage new technologies for hardware and software compromises and insertion techniques. In the updated Framework and NIICS initiatives, NIST should consider offering recommendations and capturing best practices on data system automation to meet these rapidly evolving threats.

3. Securing Data Repositories and Communications

NIST and its private sector partners (including Fortress) continue to improve the collection of SBOM and other supply chain risk data, develop more extensive data libraries, and create new tools to verify the accuracy of such data. In the course of doing so, we should expect adversaries

[5] Department of Commerce, National Telecommunications and Information Administration (NTIA), *Notice and Request for Comments on Software Bill of Materials Elements and Considerations,* Federal Register, Vol. 86, No. 104, Wednesday, June 2, 2021, pp. 29568-71.

to target vulnerabilities and attempt to corrupt the data vendors and asset owners need to manage risks. Fortress has developed increasingly stringent measures to protect the data that it holds and the systems used to collect and share that data with its clients. Fortress is also developing plans and capabilities to reinforce these security measures and stay ahead of adversarial threats. Fortress would welcome the opportunity to discuss such best practices and emerging automation opportunities.

*