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

Request for Information in response to: NIST RFI-2022-03642

Submitted to
National Institute of Standards and Technology (NIST)

Submitted by
GE Research
One Research Circle
Niskayuna, NY 12309-1027

Technical Point of Contact
Dr. Masoud Abbaszadeh
Principal Investigator
Principal Engineer
[redacted]

Business Point of Contact
Dr. Sachin Jain
Senior Manager
External Technology Partnerships
[redacted]

Date Submitted: **4/25/2022**

GE Research

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

Masoud Abbaszadeh, Stephen Bush, John Carbone, Peter Koudal, Matthew Nielsen, Walter Yund

GE Research

RE: in Response to NIST RFI-2022-03642

To whom it may concern,

In response to the RFI on NIST cybersecurity framework (CSF) and Cyber Supply Chain Risk Management (C-SCRM), hereby we are delighted to offer our comments in the following sections on cyber-physical and Industrial Control Systems (ICS) security, cybersecurity in supply chains and emerging fields of 5G, IoT and quantum computing, as they become ubiquitous in IT/OT networks, ICS and supply chains.

Cyber-Physical and ICS Security

Motivated by increasing demand for performance, availability, efficiency, and resilience, several sectors including energy, manufacturing, healthcare, and transportation have adopted latest advances in controls, automation, communications, and monitoring in the past decades, moving towards semi-autonomous or fully autonomous systems in some cases. The resulting integration of information, control, communication, and computation with physical systems, demands new methodologies for detailed systematic and modular analysis and synthesis of Cyber-Physical Systems (CPSs) to realize the desired performance metrics of efficiency, sustainability, and safety. However, CPSs suffer from extendable vulnerabilities that are beyond classical networked systems due to the tight integration of cyber and physical components. Sophisticated and malicious cyber-attacks continue to emerge to adversely impact CPS operation, resulting in performance degradation, service interruption, and system failure. Cyber-physical security provides a new line of defense at the physical domain layer (i.e., the process level) in addition to the network Information Technology (IT) and higher-level Operational Technology (OT) solutions.

In the past few years, there has been tremendous research and development efforts in cyber-physical security and resilience. The forefront of these efforts is to develop theory and technology to detect and localize cyber-attacks, identify attack types, estimate, and reconstruct attacks, and to perform secure estimation and control under attack. An example of such solutions is GE's Digital Ghost, an AI-based cyber-physical security and resilience technology for ICS and critical infrastructure, being developed at GE Research in partnership with GE business units and the Department of Energy.

Development of a cyber-physical security technology, practice and process should follow a design philosophy that includes three main aspects:

1. *Scalability:* This is itself two-fold (a) to be organically expandable to large-scale systems, and (b) to be applicable to horizontal and cross-domain applications with reasonable system modeling/dataset generation, while the core algorithms and architecture remaining domain-agnostic.
2. *Robustness:* Ability to perform in high performance (in terms of requirements such as false positive and false negative rates, speed of detection, etc.) in the presence of model uncertainty, data value and label uncertainty, as well as system's operational and configuration/manufacturing variations.
3. *Coherence:* Having a unified architecture with modularity and flexibility to identify essential and optional modules and to fit into different application domains.

In particular, we propose the following suggestions for cyber-physical and ICS security in CSF:

- NIST Guide to Industrial Control Systems (ICS): Security NIST Special Publication 800-82, should be mapped to NIST CSF.
- Cyber-physical security and process variable monitoring at the physical layer (ICS level 0-1) should be included in the NIST CSF.
- In Risk Assessment (ID.RA) – NIST should emphasize or recommend a consequence-based risk assessment approach, where "high consequence events" are prioritized for further focus. To this end, Idaho National Laboratory has a good methodology called "Consequence-driven Cyber-informed Engineering", (https://inl.gov/cce/).
- In Security Continuous Monitoring (DE.CM) – One potential addition is to define a defense in depth monitoring approach to detect abnormalities in both the cyber (network) and physical processes.

Cybersecurity in Supply Chains

The issue of cybersecurity and risk management in supply chain keep growing in importance. Cybersecurity risks and supply chain shocks can severely impact the performance of critical supply chains supporting consumer, industrial, infrastructure and defense industries. The fundamental challenge is the risk management and mitigation for complex, multi-echelon, multi-entity global supply chain networks and the latent need for secure multi-entity supply chain information, finance, materials (parts, components, bill of materials, products), and services flows.

The NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF) addresses important aspects of cybersecurity challenges with a particular focus on individual companies or organizations. In a world in which cybersecurity challenges, risks, and impacts are increasingly felt across the entire network of the supply chain for a given product or service, however, it would be beneficial to consider augmenting the CSF to address these challenges and risks and identify new ways of managing and mitigating those risks.

Given the complex, multi-entity, multi-echelon, ecosystem, and global nature of most supply chains, there is an emerging need to develop appropriate cybersecurity roadmaps, recommendations and

standards for the associated flow of information, finance, parts, product and services. This approach would suggest opportunities to address gaps in the CSF from this multi-echelon global supply chain perspective; for example, for the CSF main framework functions, an initial approach may be to consider adding relevant areas of capabilities, such as:

CSF Framework Functions and Supply Chain Cybersecurity Suggestions:

- Identify: Suggest introducing, e.g., chain of custody cybersecurity concepts for supply chain network.
- Protect: Suggest introducing, e.g., digital trust across Network Communication cybersecurity concepts for supply chain network.
- Detect: Suggest introducing, e.g., enabling multi-level threat/event detection across supply chain network.
- Recover: Suggest introducing, e.g., recovery planning and communication for supply chain network.
- Respond: Suggest introducing, e.g., multi-entity response plan execution after incident for affected supply chain network.

Furthermore, In Supply Chain Risk Management (ID.SC) – NIST should recommend that an organization analyze both hardware and software supply chains.

This approach is by no means simple and new approaches to cybersecurity risk management in global supply chains may need to be invented and framed including the leverage of new and emerging technologies in computing, communication, cryptology and other fields. But the returns on improving NIST's cybersecurity resources for improving cybersecurity in supply chains can be significant and help address a litany of challenges, risks and inefficiencies in managing and optimizing global supply chains.

Note that CSF uses the term "tier" to describe different levels of depth/maturity of CSF implementation. It would potentially be preferable to align the terminology with other cybersecurity frameworks and avoid overlapping with a term usually associated with supply chain structures – e.g., Original Equipment Manufacturer (OEM), tier 1 supplier, tier 2 supplier, etc. For example, the Department of Defense Cybersecurity Maturity Model Certification (CMMC) uses the term "level" to identify the maturity level of implementation of cybersecurity standards.

Cybersecurity in the Era of 5G, IoT, and Quantum-Resistance

As new technologies for connectivity and computing emerge, there comes new cybersecurity challenges as well as opportunities to be considered. In this section we elaborate our thoughts on cybersecurity in the face of 5G (and future generations), IoT and quantum computing.

ICS and SCADA Security Concerning Emerging Tech

A generic CPS architecture by considering the applications related to secure (ICS) to explain the cyber resilience concepts is illustrated is in the US DHS ICS-CERT recommended practice for defense-in-depth strategies and based on the Purdue five-level model. An ICS is a set of electronic devices to monitor, control, and operate the behavior of interconnected systems. ICSs receive data from remote

sensors measuring process variables, compare those values with desired values, and take necessary actions to drive (through actuators) or control the system to function at the required level of services.

Industrial networks are composed of specialized components and applications, such as programmable logic controllers (PLCs), SCADA systems, and DCS. There are other components of ICS such as remote terminal unit (RTU), intelligent electronic devices (IED), and phasor measurement units (PMU). Those devices communicate with the human–machine interface (HMI) located in the control network. However, with the rise of 5G and industrial IoT, the ICS architecture is becoming even more connected with lower-level edge devices increasingly connected to each other and to the cloud, hence, expanding the attack surface and demanding for better cybersecurity solutions. This increased connectivity and reduced latency have also enabled design of distributed architectures and distributed edge computing, creating both cybersecurity opportunities and challenges.

- As a result, considering that the Purdue model might becoming obsolete in light of the new connectivity paradigms, both NIST CSF and NIST Guide to ICS Security (800-82) should be updated to include IoT architectures over wired or wireless networks.

Supply Chain Security Concerning Emerging Tech

General Electric has concerns regarding 5G wireless communications, the Internet of Things (IoT), and quantum technology risks, elaborated below. GE encourages your consideration of these priorities and recommendations.

With respect to 5G, key performance indicators (KPI) will encourage more applications to transition from wired to wireless operation, including supply chain communication and delivery mechanisms. Applications will be spread across user equipment (UE), multiaccess edge computers (MEC), and 5G Core/Cloud. Security between and among these partitions of the 5G system is not well considered. Also, secure migration of MEC applications from one platform to another (for mobile applications) is not well addressed in the current framework. 5G Network Function Virtualization (NFV) security enhancements should be considered. We also recommend that procedures that address both classical and quantum attack vulnerabilities be included specific to 5G and NFV.

With respect to IoT, the time-sensitive networking (IEEE 802.1 TSN) suite of standards are becoming widely deployed, which allows industrial and information technology traffic [all levels of the Purdue model (ISA-99)] to coexist within the same infrastructure using scheduled end-to-end traffic flows (note that this is also occurring over 5G wireless communications). TSN can provide additional security by physically separating traffic flows but suffers from vulnerabilities to its time synchronization mechanism. This is not well addressed in the current framework. We recommend that target organizations specifically evaluate their time synchronization mechanisms for both classical and quantum attack. See GE Time-Sensitive Quantum Key Distribution (TSQKD): https://www.ge.com/research/project/time-sensitive-quantum-key-distribution for more technical information.

Finally, all security should include awareness of the transition to quantum-resistant technology; this is a concern not currently addressed in the NIST Cybersecurity Framework. Asymmetric (public key) – RSA, DH, ECC, and some Symmetric – AES, MAC, AEAD protections are at moderate to high risk. We recommend that a procedure be put in place to evaluate the supply chain's vulnerability to quantum attack and to prepare for impending mitigation. Procedures for certification of both Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD) should be developed. The overhead of PQC

and the need to integrate QKD into devices are examples of concerns that should be considered. See GE Time-Sensitive Quantum Key Distribution (TSQKD): https://www.ge.com/research/project/time-sensitive-quantum-key-distribution. ETSI QKD standards and profiles must be included in the NIST Framework https://www.etsi.org/committee/qkd.