INL/EXT-21-64089
Revision 0

Towards a New Supply Chain Cybersecurity Risk Analysis Technique

August 2021

FY21 DOE-NE Cybersecurity Supply Chain Research Report

Shannon Eggers
Idaho National Laboratory

Idaho National Laboratory

*INL is a U.S. Department of Energy National Laboratory
operated by Batelle Energy Alliance, LLC*

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/EXT-21-64089
Revision 0

Towards a New Supply Chain Cybersecurity Risk Analysis Technique

FY21 DOE-NE Cybersecurity Supply Chain Research Report

Shannon Eggers
Idaho National Laboratory

August 2021

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of Nuclear Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Page intentionally left blank

ABSTRACT

Supply chain cyber-attacks, such as the SolarWinds Orion attack, are occurring with greater frequency. These attacks compromise a digital device before it is sent to customers, bypassing traditional security controls to remain persistent and undetected in operational environments. While supply chain attacks are prevalent, methods for analyzing the risk of these attacks are currently unavailable. This paper proposes new supply chain cyber-attack difficulty and risk metrics to evaluate the relative risk of an attack throughout the supply chain lifecycle. Difficulty metrics for each stakeholder in a digital device's supply chain (e.g., hardware manufacturing, firmware development, software development, storage, and distribution entities) are calculated using scores from cybersecurity maturity questionnaires in a Bayesian Network leaky Noisy-MAX model. These difficulty metrics are then used to calculate an overall supply chain cyber-attack risk. Vulnerability and recoverability metrics are also proposed to evaluate the relative stakeholder influence in the attack risk. These proposed relative risk metrics enable continuous supply chain monitoring, provide decision-makers with information necessary for improved supplier selection, and help drive improvements in the cybersecurity posture of the stakeholders in their supply chain.

Page intentionally left blank

ACKNOWLEDGEMENTS

This work was supported by the U.S. Department of Energy Office of Nuclear Energy Cybersecurity Crosscutting Technology Development program under the DOE Idaho Operations Office, Contract DE-AC07-05ID14517.

Page intentionally left blank

CONTENTS

FIGURES

TABLES

Page intentionally left blank

Towards a New Supply Chain Cybersecurity Risk Analysis Technique

1 INTRODUCTION

In an operational technology (OT) environment, such as a nuclear power plant (NPP), cyber threat vectors include wired and wireless networks, insiders, portable media and mobile devices (PMMD) (e.g., maintenance laptops, USB drives), and the supply chain. Implementations of secure architectures, including use of deterministic data diodes, improved insider threat mitigation programs, and PMMD administrative policies have reduced cyber risks in critical infrastructure facilities. However, due to the difficulty in securing the complex global supply chain network, it remains vulnerable.

And, while recent high-profile supply chain attacks, such as the SolarWinds Orion attack, have caused shockwaves through the information and communications technology (ICT) industry, the supply chain for OT devices may be considerably larger than a software supply chain; it may include geographically dispersed designers, hardware manufacturers, firmware developers, software developers, and integrators, as well as physical and electronic storage and distribution entities. Although many standards and guidelines on cyber supply chain risk have been written (refer to Section 3.2), there are not any actionable supply chain cybersecurity risk analysis methods available to evaluate overall risk. This paper proposes new cybersecurity risk metrics for supply chain analysis, including attack difficulty, attack risk, vulnerability, and recoverability. The goal is to improve overall awareness into a device's supply chain to enable continuous risk reduction by informing supply chain decisions and enhancing cybersecurity posture throughout the supply chain.

The remainder of this paper is organized as follows: Section 2 provides a background on traditional supply chain risk management. Section 3 provides a background on cyber supply chain risk management, including supply chain cybersecurity risk analysis, cyber supply chain standards and guidelines, and the use of Bayesian Networks (BN) in supply chains. Section 4 details the proposed cybersecurity supply chain metrics, while Section 5 provides examples of their use. A discussion is provided in Section 6 prior to conclusions in Section 7.

2 TRADITIONAL SUPPLY CHAIN RISK MANAGEMENT

OT devices, including digital instrumentation and control (I&C) systems and components, are used throughout NPPs. The number of digital systems, structures, and components (SSCs) in NPPs will continue to increase with plant modernization initiatives and construction of new advanced reactors. Supply chain management (SCM) for OT devices is concerned with the flow of hardware, firmware, and software throughout the product lifecycle from design to manufacturing, assembly, installation, maintenance, and repair. In general, risk management is the process of identifying or analyzing risks, evaluating the identified risks against risk tolerance levels, and responding to the risks by either eliminating, transferring, accepting, or mitigating the risk. As shown in Figure 1, traditional supply chain risk management (SCRM) balances SCM objectives of cost minimization, quality, and availability against potential disruptions from environmental, geopolitical, and financial elements.

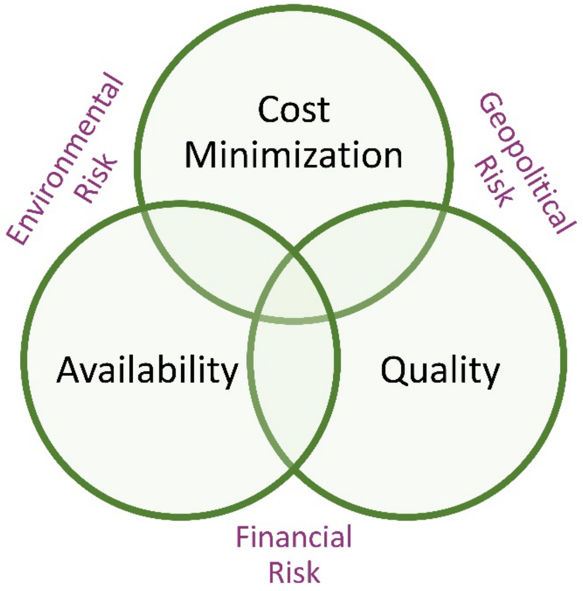


Figure 1. Traditional SCRM objectives and risks.

Based on Kaplan and Garrick's risk definition in which risk is a function of the scenario, likelihood, and consequence [1], traditional supply chain risk analysis considers the likelihood of a given scenario (i.e., environmental, geopolitical, or financial disruption) causing an adverse consequence (i.e., negatively impact the SCM objectives). As shown in Figure 2, quality is often evaluated based upon product reliability, completeness, authenticity, and accuracy while availability is based upon resiliency, dependability, survivability, and robustness of product delivery. Many costs exist throughout a supply chain, including stakeholder costs, material costs, logistics costs, and inventory costs.

In today's global economy, the OT supply chain consists of multiple tiers of geographically dispersed stakeholders, regardless of whether the product is a single device or a complex control system. Stakeholders, as used in this paper, indicate all entities involved in the supply chain, such as suppliers, designers, shippers, warehouses, and integrators. While an expansive international supply chain increases competition, reduces sub-component costs, and accelerates production times, the additional complexity also intensifies a company's exposure to external threats. If materialized, these threats could raise costs from accompanying problems, such as reduced quality or missed deadlines from manufacturers, software developers, or logistics providers.

Notwithstanding potential internal threats (e.g., those within the end-user's control), external supply-related threats in traditional SCRM include environmental, geopolitical, and financial risks. As shown in Figure 2, environmental risk includes disturbances such as natural disasters, ecological disasters, weather events, and pandemics. Geopolitical risk, includes disturbances, such as political instability, trade restrictions, corruption, criminal activity, terrorism, and civil unrest, are increasingly more likely as global trade activities expand. Financial risk, like price volatility, demand shocks, transportation or border delays, regulatory issues, legal challenges, and exchange rate or currency fluctuations.

By evaluating the potential supply chain disruptions or events, the likelihood of these events, and their possible impact on product cost, availability, and quality, a company can identify and prioritize risks based upon their risk tolerance and then respond by either eliminating, accepting, transferring, or mitigating the risk. Often, risk-informed cost-benefit analyses are used to optimize risk response and reduce overall vulnerability to supply chain disruptions. The ultimate goal is a resilient, reliable, and available supply chain in which disruptions are avoided or minimized, costs are minimized, and quality is maximized [2].

3 CYBER SUPPLY CHAIN RISK MANAGEMENT

Figure 2 expands on the traditional SCRM in Figure 1 to provide a Cyber SCRM (CSCRM) framework that includes security objectives and the inherent cyber-physical threats for OT supply chains. Failure to recognize and evaluate the risks associated with deliberate, malicious cyber incidents potentially exposes stakeholders and end-users to unmitigated risk. The traditional SCRM objections and external threats were discussed in the prior section. The security objectives and cyber-physical threats for OT supply chains are discussed in the following sections.

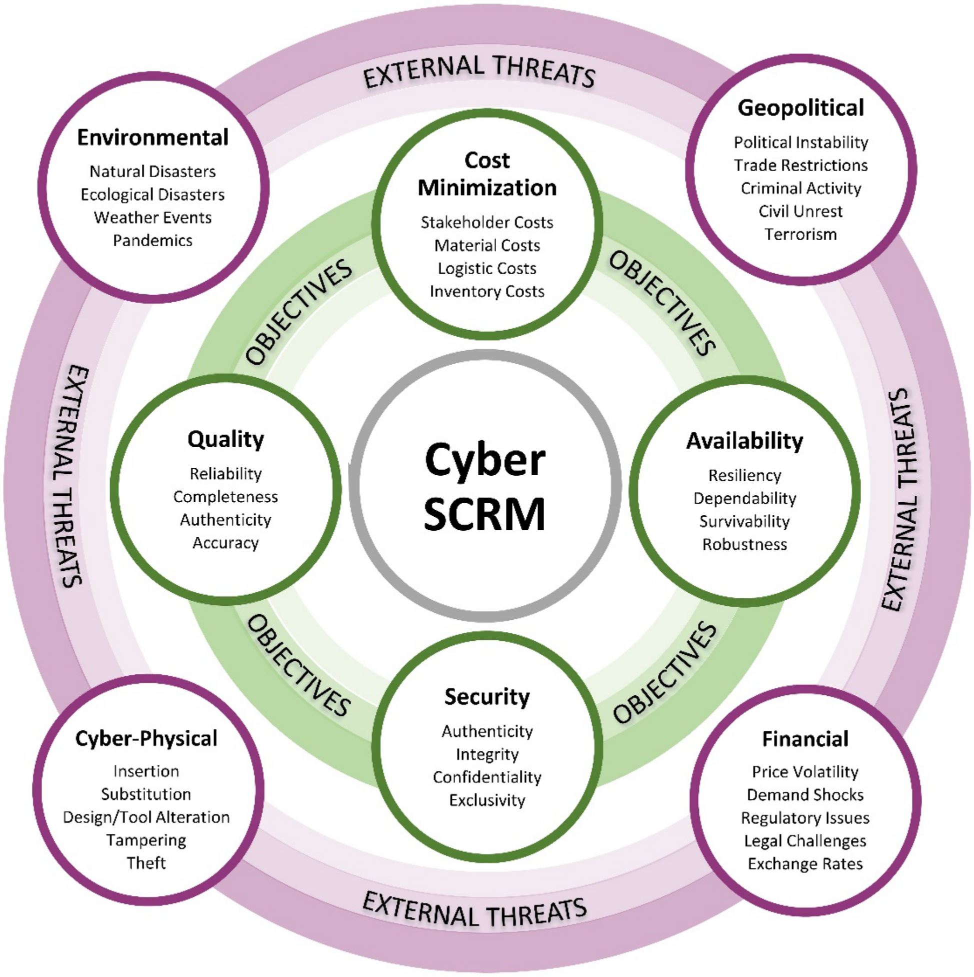


Figure 2. Cyber SCRM framework for OT supply chains.

3.1 Supply Chain Cybersecurity Risk Analysis

Whereas Kaplan and Garrick identified risk using a <scenario, likelihood, consequence> triplet, cyber risk in operational environments may be more effectively identified using a <threat, vulnerability, consequence> triplet [1]. Narrowing the scope of CSCRM to focus solely on security, this same cyber risk triplet can be applied to supply chain cybersecurity risk analysis. It is noted that cyber risk considers a broad set of threats, including both adversarial and unintentional actions (e.g., device failures or human performance errors), while cybersecurity risk considers the smaller subset of adversarial threats. Since the 'quality' SCRM objective incorporates unintentional actions, such as design or manufacturing flaws, this paper adopts the cybersecurity viewpoint and limits the analysis to adversarial cyber-physical threats in the supply chain.

3.1.1 Threat

Adversarial threat includes the potential of cyber-attack by a bad actor. There are several taxonomies of supply chain cyber-attacks [2-5]. The following paragraphs summarize the six high-level attack types from [4].

Malicious substitution and counterfeiting involve the complete replacement of hardware (including firmware) or software with a non-authentic replacement. Oftentimes, counterfeits are produced by reverse engineering a product or stealing design information, such as intellectual property (IP). While many counterfeits are produced and sold for financial gain rather than to maliciously impact operations, any substitution is a nonconformance that can potentially adversely affect facility functions.

Compromises consisting of malicious insertion involve the intentional addition or modification of hardware, firmware, or software with the intent to adversely impact device operation. Tampering, on the other hand, is the unauthorized alteration of configuration, including hardware, firmware, or software configuration. As defined, tampering does not involve modifications to executable code or data.

Theft of IP, design, data, or other system information, such as stored secrets, can occur throughout the supply chain lifecycle. In addition to enabling counterfeiting, theft of system information can enable development of more sophisticated attacks and/or result in other economic losses. Other lesser-considered attacks include alteration of design information or development tools. Unauthorized modification of system information (e.g., design, specification, requirements) may result in development of products that include latent design deficiencies or vulnerabilities, such as the inclusion of back-doors. Similarly, unauthorized modification of development, build, or programming tools may result in product corruption.

3.1.2 Vulnerability

Vulnerabilities are weaknesses that can be intentionally (or accidentally) exploited or misused. OT vulnerabilities are often identified by evaluation of an attack surface defined as a “set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment.” [6] The cyber supply chain also has an attack surface. The OT supply chain cyber-attack surface is the sum of the complex network of stakeholders and activities involved in the supply chain lifecycle for the entire digital bill of materials, including hardware, firmware, software, and system information [7].

Each of the stakeholders and touchpoints involved in the lifecycle has its own set of vulnerabilities, those weaknesses in physical and electronic security that can be exploited by an adversary. For instance, a hardware integrator may have poor physical security, enabling tampering of a component, while a software developer may have poor IT security, enabling insertion of malware into a software application via the internet.

3.1.3 Consequence

In operational OT environments (e.g., NPP I&C systems), cybersecurity objectives are often defined using the C—I—A triad (confidentiality—integrity—availability), where the goal of confidentiality is to ensure information privacy and prevent unauthorized access of information, the goal of integrity is to ensure trustworthiness by maintaining accurate and complete data, and the goal of availability is to ensure there are no disruptions in systems or functions. Similarly, cyber supply chain security objectives are often defined in terms of AICE [7, 8] as shown in Figure 2, where:

Authenticity = Genuine, unsubstituted, not counterfeit

Integrity = Trustworthy, untainted, uncompromised

Confidentiality = No unauthorized transfer of information, data, or secrets

Exclusivity = Limited possession, control, or use by authorized stakeholders

Like traditional SCRM objectives, the four objectives in CSCRM—security, quality, availability, and cost minimization—are often interrelated. For instance, a stakeholder that has poor cybersecurity hygiene is at risk for product compromise, thereby potentially affecting product quality. Conversely, improvements in a stakeholder's cybersecurity posture may result in higher costs and slower development or production timelines due to added security constraints, which may impact product costs and availability. Of course, a supply chain cyber-attack will likely also adversely impact facility functions upon installation and operation.

3.1.4 Likelihood

Traditional risk analysis techniques include likelihood, or the probability that a scenario will occur. Likelihood is difficult, if not impossible, to determine in cyber risk largely due to unknown unknowns, both adversarial and unintentional. For instance, digital equipment often fails in unexpected ways, threats and vulnerabilities constantly change, and human actions are unpredictable. Likelihood is also challenging to determine in physical security for similar reasons. Since stakeholders in the supply chain may be compromised by physical, cyber, or hybrid attacks (e.g., physical-cyber attacks), determining the likelihood of a supply chain attack with any reasonable level of certainty is most likely impossible.

To overcome this challenge, several techniques have explored using variations of attack difficulty as an alternative to likelihood. The Risk-Informed Management of Enterprise Security (RIMES) methodology uses degree of attack difficulty rather than attack likelihood for physical security risk analysis of nuclear facilities [9, 10]. The Electric Power Research Institute (EPRI) Technical Assessment Methodology [11], Systems Theoretic Process Analysis (STPA)-informed risk matrix technique [12], and NUREG/CR-6847 [13] use mitigation or protection effectiveness to analyze whether risk is reduced when control or countermeasures are implemented.

3.2 Cyber Supply Chain Standards and Guidelines

In prior surveys of risk assessment standards, it was concluded that standards used for OT risk assessments are too high-level and do not capture the specificities of critical energy infrastructures [14-16]. Similarly, even though it is recognized there is ongoing activity and research to improve the cyber supply chain, the current cyber supply chain standards and guidelines are insufficient to secure industrial control systems (ICS) within critical sectors. In fact, Nissen et al. state that while there is general awareness of supply chain threats, risk management is given insufficient resources, there is too little attention to operational security, and threat information is siloed such that risk-informed decision analysis is inadequate [17]. Although this 'Deliver Uncompromised' report is focused on the Department of Defense (DoD) acquisition process, the conclusions reached in this report can be extended to the larger ICS community.

Table 1 lists a selection of relevant cyber supply chain standards, guidelines, or instructions by domain. These high-level conceptual documents address various cyber supply chain mitigation topics, such as counterfeit avoidance, cyber procurement language, anti-tamper requirements, secure software/system development, and information protection, but none of them adequately identify a methodology for assessing cyber supply chain risk or how to measure mitigation effectiveness.

Table 1. Selection of cyber supply chain standards and guidance by domain.

Domain	Publication
Aerospace	SAE AS5553C, Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition [18] SAE AS6081, Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition-Distributors [19] SAE ARP9134A, Supply Chain Risk Management Guideline [20]
Defense	DoDI 5000.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks [21] Defense Acquisition Guidebook, Chapter 9—Program Protection [22] DFARS 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System [23] DFARS 252.246-7008, Sources of Electronic Parts [24] DoDi 5000.02, Operation of the Defense Acquisition System [25] DoDD 5200.47E, Anti-Tamper [26] Cybersecurity Maturity Model Certification (CMMC) [27]
Energy	DOE Cybersecurity Capability Maturity Model (C2M2) [28] EPRI Cyber Security Procurement Methodology for Power Delivery Systems [29] ESCSWG, Cybersecurity Procurement Language for Energy Delivery Systems [30] NERC CIP-013-1, Cyber Security-Supply Chain Risk Management [31]
Nuclear	EPRI Cyber Security in the Supply Chain: Cyber Security Procurement Methodology [32] EPRI Secure Development, Integration, and Delivery (SDID) Audit Topical Guide [33] NEI 08-09 Addendum 3, Cyber Security Plan for Nuclear Power Reactors, Systems and Services Acquisition [34]
ICS	DHS Cyber Security Vendor Procurement Language for Control Systems [35] IEC 62443-2-4, Security Program Requirements for IACS Solution Suppliers [36] IEC 62443-4-1, Secure Product Development Lifecycle Requirements [37] UL 2900-2-2, Part 2-2, Particular Requirements for Industrial Control Systems [38]
ICT	CISA, Vendor Supply Chain Risk Management (SCRM) Template [39] CISA, Threat Evaluation Working Group: Supplier, products, and services threat evaluation [5] CISA, Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists [40] ENISA Threat Landscape for Supply Chain Attacks [2] ISO/IEC 27036-3, Information Security for Supplier Relationships, Part 3, Guidelines for ICT Supply Chain Security [41] ISO/IEC 20243-1, Information Technology-O-TTPS-Mitigating maliciously tainted and counterfeit products [42] NISTIR 7622, Notional Supply Chain Risk Management Practices for Federal Information Systems [43] NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security [44] NIST SP 800-147, BIOS Protection Guidelines [45] NIST SP 800-147b, BIOS Protection Guidelines for Servers [46] NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations [47] UL 2900-1, Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements [48]
Software	SAFECode, Fundamental Practices for Secure Software Development [49] SAFECode, The Framework for Software Supply Chain Integrity [50] SAFECode, Managing Security Risk Inherent in the use of Third-Party Components [51] CISA, Defending Against Software Supply Chain Attacks [52]

3.3 Bayesian Networks in Supply Chain Risk Management

A BN is a directed acyclic graph used for combining subjective beliefs with available evidence to develop probabilistic graphical models. BNs have been used for risk analysis, uncertainty modeling, and decision-making. A BN is comprised of parent and child nodes in which conditional dependencies between parent and child are described by a conditional probability table (CPT) at each child node and unconditional probabilities or prior probabilities are specified at root nodes (i.e., nodes without parents). BNs can be used to estimate the probability distributions in a top-down or bottom up-method in large networks where data is uncertain or incomplete.

Pai et al. first proposed a BN methodology for assessing risk and evaluating safeguards to secure the supply chain [53]. Researchers have also used BN to model dependencies between suppliers and manufactures to evaluate environmental disruptions on manufacturer performance [54]. However, applying BN to practical problems is challenging because a complete CPT for a binary variable increases exponentially with the number of parent variables (e.g., full specification of a child with *n* binary parents requires 2^n independent parameters). To simplify these complex CPTs, Barker and Hosseini investigated using the BN canonical gate leaky Noisy-OR model to develop a supply chain resilience metric based on vulnerability and recoverability scores [55, 56]. The vulnerability metric measures the percentage of increase on manufacturing disruption risk when a supplier is disrupted (i.e., evidence describing the supplier is entered and set to True). The recoverability metric measures the decrease in manufacturing disruption risk when the supplier is fully operational (i.e., evidence describing the supplier is entered as 100% False).

The leaky Noisy-OR model is useful for large networks because it reduces computational complexity and is useful for approximating the relationships in practical applications; the exponential requirement for full elicitation reduces to a linear requirement [57]. It should be noted, however, that the presence of conditional inter-causal independence in the leaky Noisy-OR model results in the absence of the BN 'explaining away behavior' in backward inference when the effect variable is observed as False [58]. Díez proposed a parameterization of the Noisy-OR gates to model interactions among variables with multiple states [59, 60]. In this leaky Noisy-MAX model, the net CPT for a child node expresses the probability of an effect happening when the parent cause is present and none of the other parent causes are present.

4 PROPOSED CYBERSECURITY SUPPLY CHAIN METRICS

Critical digital assets (CDAs) required to remain functional to maintain essential safety- or business-critical objectives in OT environments are typically identified through a facility's cybersecurity program. Thus, our supply chain risk analysis technique assumes that the digital asset analyzed is a CDA and that a cyber-attack to the CDA will cause adverse impact to the facility. While consequences of a supply chain attack during operational phases may vary depending on what component is compromised and how it is compromised, consequence is not further analyzed in this study.

Recognizing that likelihood is challenging to determine in cybersecurity supply chain risk analysis without high degrees of uncertainty, we propose a new supply chain difficulty metric. A successful supply chain cyber-attack will be less likely if an entity has an advanced cyber security program in place with effective organizational, protective, detection, and response capabilities. In other words, an attack will be more difficult against a stakeholder with better security.

We propose establishing a cybersecurity supply chain difficulty metric for a stakeholder by first defining cybersecurity ratings for (1) organizational capability, (2) protection and prevention capability, and (3) detection and response capability, where the stakeholder's cybersecurity capabilities are rated on a scale from 1 to 5, with 1 indicating very poor security and 5 indicating very good security.

Several guidelines have been developed to assess the cybersecurity maturity level of a stakeholder, including the DOE Cybersecurity Capability Maturity Model (C2M2) [28], the DoD Cybersecurity Maturity Model Certification (CMMC) [27], and the CISA Vendor Supply Chain Risk Management Template [39]. The CISA Vendor Supply Chain Risk Management Template is included in Annex A as an example. Additionally, an asset owner can certify their sites or systems to IEC 62243 standards or certify their products as IEC 62443 or UL 2900 compliant. The maturity level ratings for these publications are mapped to the new stakeholder cybersecurity capability rating, as indicated in Table 2.

Table 2. Guideline/standard maturity level rating mapped to the capability rating.

Capability Rating*	C2M2 Rating	CMMC Rating	CISA SCRM Template	IEC 62443 & CMMI
Very Poor	MIL1	Basic	Level 1	Initial
Poor		Intermediate	Level 2	Managed
Moderate	MIL2	Good	Level 3	Defined/Practiced
Good		Advanced	Level 4	Improving
Very Good	MIL3	Proactive	Level 5	

* Supply cybersecurity capability rating for the method defined in this paper.

In general, the questions in these guidelines or certifications can be categorized into the three defined stakeholder cybersecurity capabilities. Figure 3 provides a notional breakdown of question categories for each capability.

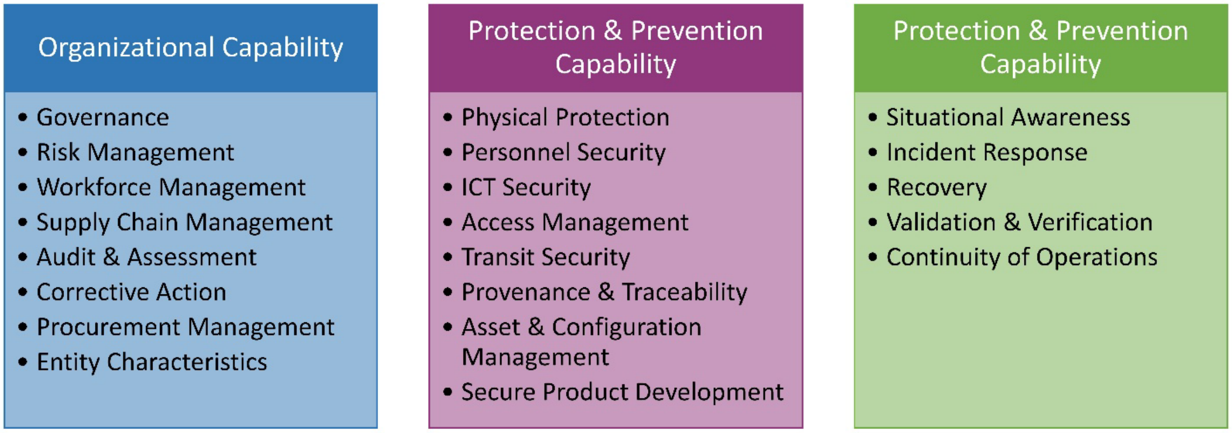


Figure 3. Notional categorization of question type by stakeholder cybersecurity capability.

Although a unique questionnaire based on existing guidelines may prove more effective in the long-term, the intent of this initial investigation was to develop a ‘questionnaire agnostic’ methodology with the underlying assumption that the chosen guideline incorporated an appropriately sized set of relevant questions to provide a score in each of the three categories. Third-party certification or attestation will likely provide more accurate answers to the questions. As part of this study, questionnaire mappings for the DOE C2M2, DoD CMMC, and CISA Vendor SCRM guidelines have been developed. Table 3 is an example of maturity level scores aggregated by capability based upon an information security benchmark dataset of ICT company responses from the Information Technology Protection Agency (IPA) [61]. It is recognized that questions may be highly correlated or may fall into multiple capability categories. Since the intent is to develop a relative stakeholder attack difficulty metric, this possibility is not addressed in this study.

Table 3. Average capability scores calculated from the 2020 IPA Information Security Measures Benchmark for ICT companies [61].

Capability	Average Respondent Score per Capability (Scale 1 to 5)
Organizational Capability	3.186
Protection/Prevention Capability	3.385
Detection/Response Capability	3.156

Consider a simple supply chain for a CDA (X) that includes a hardware (HW), firmware (FW), and software (SW) supplier, as represented by the BN in Figure 4. There exists a probability that a sub-component will be attacked at either a HW, FW, or SW supplier leading to a compromised CDA. As the supply chain cyber-attack surface may be extensive and include numerous other nodes, such as integrators, physical and electronic storage locations, and distribution pathways [7], constructing BN CPTs to model compromise of a CDA is challenging. To simplify the model construction, we used the Noisy-MAX model as described by Díez in which the number of parameters is proportional to the number of causes instead of exponential as seen in the general BN case [60].

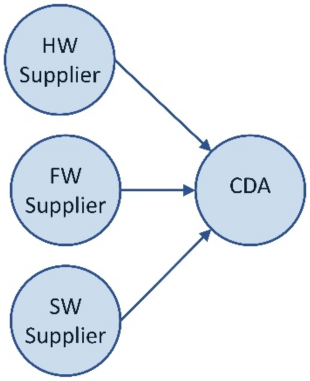


Figure 4. A simple supply chain BN with three suppliers (S) and one CDA (X).

In the leaky Noisy-MAX model, it is assumed there is a probability associated with a supply chain CDA (X) attack successfully occurring when one and only one supplier (S) is attacked, and all other suppliers are not attacked, as expressed by:

$$NoisyMAX(S_1, u_{X|S_1}, S_2, u_{X|S_2}, \dots, S_n, u_{X|S_n}, L_X) \tag{1}$$

where for each $i, u_{X|S_1} = P(X^{Attack}, S_i^{NotDifficult}, S_j^{Difficult}\ for\ each\ j\ \neq i)$ is the conditional probability of the CDA being attacked if and only if the i^{th} supplier has a True attack difficulty state (e.g., NotDifficult) and the other suppliers have a False attack difficulty state (e.g., Difficult). The leak variable, L_X, represents the possibility of successful CDA compromise when all suppliers have a False attack difficulty state, as expressed by:

$$L_X = P(X^{Attack}|S_1^{NotDifficult}, S_2^{NotDifficult}, \dots, S_n^{NotDifficult}) \tag{2}$$

Now consider that supplier cybersecurity capability categories are included to calculate the attack difficulty at each supplier. Thus, the attack difficulty metric for each supplier is conditional on the capability nodes, as expressed by this Noisy-MAX model:

$$NoisyMAX(C_1, u_{S|C_1}, C_2, u_{S|C_2}, \dots, C_n, u_{S|C_n}, L_S) \tag{3}$$

where for each $i, u_{S|C_1} = P(S^{Difficult}, C_i^{VeryGood}, C_j^{VeryGood}\ for\ each\ j\ \neq i)$ is the conditional probability of the supplier having a True attack difficulty state if and only if the i^{th} capability has a VeryGood state.

From [55, 56], the vulnerability score is found by calculating the percent increase on CDA attack risk when the supplier has attack difficulty set to True (e.g., 100% NotDifficult) over the CDA attack risk calculated using prior baseline probabilities. Similarly, the recoverability score can be determined based upon the supplier's attack difficulty set to False (e.g., 100% Difficult) and calculating the decrease on CDA attack risk when compared to baseline probabilities.

5 RESULTS

5.1 Simple Supply Chain Example

This hypothetical example uses the simple supply chain concept with three suppliers supplying components for one CDA as illustrated in Figure 5. Each supplier's attack difficulty level is determined by three capability nodes—organizational capability, protection capability, and detection capability. For this simple example, it is assumed there are no other nodes present.

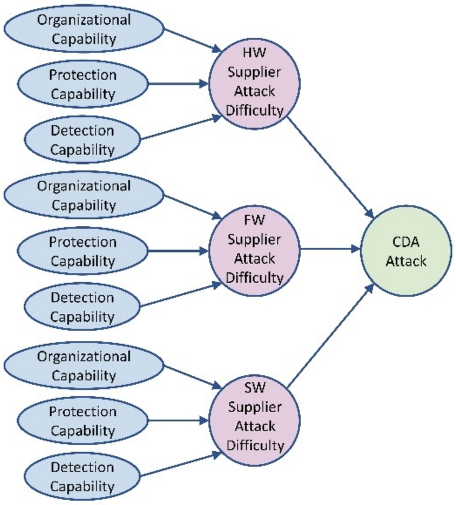

Organizational Capability
Protection Capability
Detection Capability
HW Supplier Attack Difficulty
Organizational Capability
Protection Capability
Detection Capability
FW Supplier Attack Difficulty
CDA Attack
Organizational Capability
Protection Capability
Detection Capability
SW Supplier Attack Difficulty

Figure 5. BN structure used in the attack difficulty metric study.

While the prevalence of supply chain attacks on OT devices is increasing, the current probability of such an attack successfully occurring, regardless of attack difficulty, is unknown. As such, as shown in Table 4, the conditional probabilities of a CDA attack successfully occurring if and only if the indicated supplier has a True attack difficulty state (e.g., 100% NotDifficult) are set to $\tilde{u}^{HW} = 0.05$, $\tilde{u}^{FW} = 0.10$, and $\tilde{u}^{SW} = 0.35$ in a Noisy-MAX structure, where $\tilde{u}^{S} = u_{X|S}$. These conditional probabilities, which are hypothesized based on expert opinion, indicate that a software supply chain attack is more likely than a firmware or hardware attack. The leak probability is set to 0.01 suggesting that a supply chain attack has a 1.0% probability of successfully occurring even if the attack difficulty state is False for all suppliers (e.g., 100% Difficult).

Table 4. Noisy-MAX conditional probability net table for the CDA Attack node.

Parent	**Difficulty_HW**	**Difficulty_FW**	**Difficulty_SW**	**Leak**
State	**NotDifficult**	**NotDifficult**	**NotDifficult**	
Attack	0.05	0.10	0.35	0.01
NoAttack	0.95	0.90	0.65	0.99

The difficulty metric for each supplier node was similarly established as a Noisy-MAX structure by using prior probabilities of capability ratings (e.g., Very Poor, Poor, Moderate, Good, Very Good) along with the conditional probabilities as shown in Table 5. This structure was repeated for all three suppliers. It should be noted that both the attack and difficulty conditional probabilities are hypothetical assumptions based on expert opinion and can be more accurately determined through expert elicitation. Additional research may also provide insight into attack probabilities between supplier types. In this study, the SW supplier and protection capability are weighted higher than the other factors.

Table 5. Noisy-MAX conditional probability net table for the Supplier Difficulty nodes.

Parent	Organizational Capability					Protection Capability					Detection Capability					
State	Very Poor	Poor	Mod	Good	Very Good	Very Poor	Poor	Mod	Good	Very Good	Very Poor	Poor	Mod	Good	Very Good	Leak
NotDiificult	0.50	0.30	0.10	0.05	0.00	0.85	0.55	0.25	0.05	0.00	0.65	0.40	0.15	0.05	0.00	0.02
Difficult	0.50	0.70	0.90	0.95	1.00	0.15	0.45	0.75	0.95	1.00	0.35	0.60	0.85	0.95	1.00	0.98

By mapping supply chain cybersecurity questionnaires into this model, the relative risk of a supply chain cyber-attack can be calculated and evaluated over time as security improves or threats change. For illustrative purposes, assume the capability ratings shown in Table 6 are determined by third-party supplier certifications. As indicated, the SW supplier has poor security, resulting in a low difficulty score and CDA attack probability of 31.6%.

Table 6. BN analysis results of difficulty and attack risk based upon initial capability ratings.

Supplier	Capability Rating		Difficulty Metric	
HW	Organizational	VeryGood	79.9% Difficulty	
	Protection	Good		
	Detection	Moderate		
FW	Organizational	Good	75.9% Difficulty	**CDA Attack Risk = 31.6%**
	Protection	Good		
	Detection	Moderate		
SW	Organizational	Poor	18.7% Difficulty	
	Protection	Poor		
	Detection	Poor		

Consider that the software supplier invests money and time into improving their cybersecurity program which results in improvement to all their capability ratings as shown in Table 7. The improvements to their security program reduced overall relative CDA supply chain attack probability by 20.5%.

Table 7. BN analysis results of difficulty and attack risk based upon final capability ratings.

Supplier	Capability	Rating	Difficulty Metric	
HW	Organizational	Very Good	79.9% Difficulty	
	Protection	Good		
	Detection	Moderate		
FW	Organizational	Good	75.9% Difficulty	**CDA Attack Risk = 11.1%**
	Protection	Good		
	Detection	Moderate		
SW	Organizational	Very Good	79.9% Difficulty	
	Protection	Good		
	Detection	Moderate		

Further, the vulnerability and recoverability scores for each supplier can be calculated, providing an awareness into which nodes have greater influence on supply chain attack risk. For illustrative purposes only, capability averages from Table 3 were used to set the initial evidence for each security capability to Moderate for all suppliers (HW, FW, and SW). Given this prior evidence, calculation of the model results in difficulty level of 56.8% for each supplier with a conditional probability of a CDA attack successfully occurring of 21.3%. Using this initial baseline data, the results of the vulnerability and recoverability calculations for each supplier are shown in Table 8. Similar to the previous results, this data suggests that the SW supplier has a strong influence on CDA attack risk in this model when compared to the other suppliers. The vulnerability score for the SW supplier is 18.4% indicating that when this node has no cybersecurity in place (State=True, NotDifficult = 0%), the attack risk increases by 18.4%. Conversely, the recoverability score is 14.0%, indicating that when this node has excellent cybersecurity (State=False, Difficult = 100%), the attack risk decreases by 14.0%.

Table 8. Vulnerability and recoverability scores for the simple supply chain example.

Supplier	Vulnerability Score	Recoverability Score
HW	$V(X^{attack}\|\tilde{u}^{HW}) = 0.2362 - 0.2133 = 0.0229$	$R(X^{attack}\|\tilde{u}^{HW}) = 0.2133 - 0.1960 = 0.0173$
FW	$V(X^{attack}\|\tilde{u}^{FW}) = 0.2600 - 0.2133 = 0.0467$	$R(X^{attack}\|\tilde{u}^{FW}) = 0.2133 - 0.1778 = 0.0355$
SW	$V(X^{attack}\|\tilde{u}^{SW}) = 0.3976 - 0.2133 = 0.1843$	$R(X^{attack}\|\tilde{u}^{SW}) = 0.2133 - 0.0732 = 0.1401$

5.2 Intelligent Transmitter Example

A notional block diagram of an intelligent transmitter from [7] is shown in Figure 6. Although these transmitters are relatively simple devices, there may be numerous stakeholders involved in their development, manufacturing, and assembly. An illustration of a notional BN for the HW, FW, and SW component stakeholders involved in the intelligent transmitter's supply chain lifecycle is shown in Figure 7. In addition to the HW, FW, and SW developers, this BN also includes integrators (INT), physical storage (WH), physical distribution (TX), and electronic storage and distribution (ESD) nodes. In a full real-life example, there may also be nodes for design, testing, installation, and maintenance lifecycle phases.

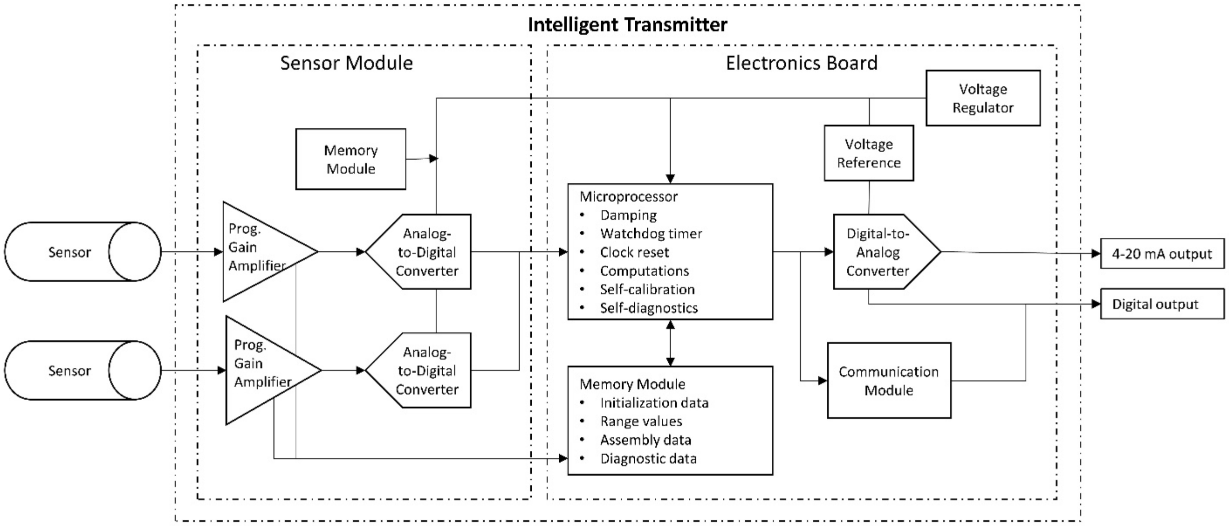


Figure 6. Notional block diagram of an intelligent transmitter from [7].

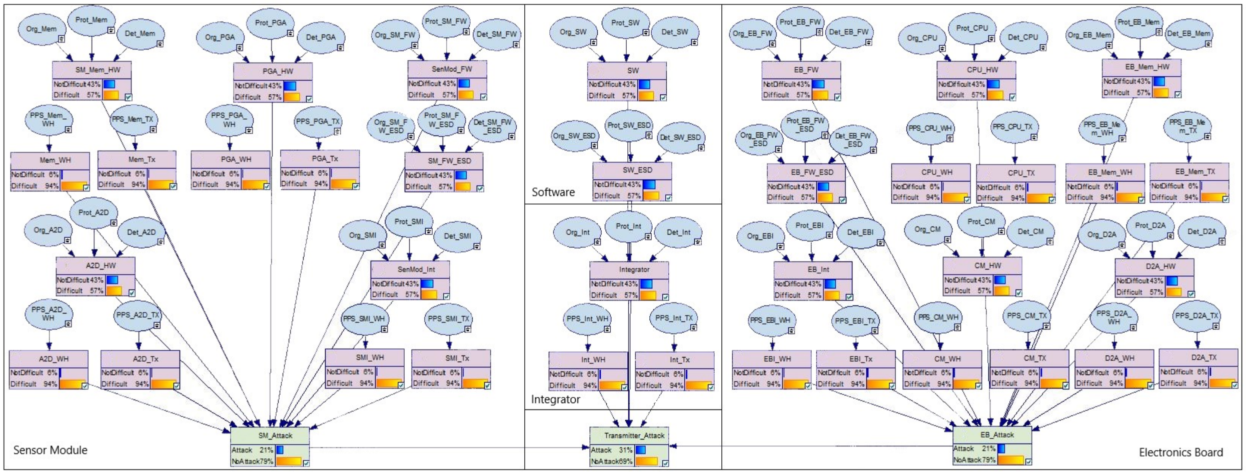


Figure 7. BN for the intelligent transmitter example.

The attack risk is first determined independently for the sensor module (SM) and electronics board (EB). The overall CDA attack risk for the completely assembled transmitter includes the SM risk, EB risk, SW developer difficulty score, and final integrator difficulty score. Setting all cybersecurity-based operational, protection, and detection capability nodes to Moderate and all the physical-security-based capability nodes for physical storage and transport to Good, results in a transmitter attack risk of 34.1%, indicating that given the prior evidence and conditional probabilities for difficulty and attack, the transmitter has a 34.1% relative risk of successful attack.

The vulnerability and recoverability scores, given the initial baseline evidence, are listed in Table 9. These results suggest the high influence of the SW and SW_ESD nodes. The SW and SW_ESD nodes increase attack risk by 15.44% when there is no cybersecurity and it is easy for an attack to successfully occur (e.g., State = True, NotDifficult = 0%). Conversely, when there is excellent cybersecurity at the SW and SW_ESD nodes (e.g., State = False, Difficult = 100%) the attack risk decreases by 11.75%.

Table 9. Vulnerability and recoverability scores for the intelligent transmitter example.

Node	Vulnerability Score	Recoverability Score
SW_Mem_HW	0.07%	0.06%
Mem_WH	0.12%	0.01%
Mem_Tx	0.12%	0.01%
PGA_HW	0.07%	0.06%
PGA_WH	0.12%	0.01%
PGA_Tx	0.12%	0.01%
A2D_HW	0.07%	0.06%
A2D_WH	0.12%	0.01%
A2D_Tx	0.12%	0.01%
Sen_Mod_FW	0.15%	0.12%
SM_FW_ESD	0.15%	0.12%
Sen_Mod_Int	0.15%	0.12%
SMI_WH	0.25%	0.01%
SMI_Tx	0.25%	0.01%
SW	15.44%	11.75%
SW_ESD	15.44%	11.75%
Integrator	3.91%	2.98%
Int_WH	6.24%	0.40%
Int_Tx	6.24%	0.40%
EB_FW	0.15%	0.12%
EB_FW_ESD	0.15%	0.12%
EB_Int	0.15%	0.12%

Node	Vulnerability Score	Recoverability Score
EBI_WH	0.24%	0.01%
EBI_Tx	0.24%	0.01%
CPU_HW	0.07%	0.06%
CPU_WH	0.12%	0.01%
CPU_Tx	0.12%	0.01%
CM_HW	0.07%	0.06%
CM_WH	0.12%	0.01%
CM_Tx	0.12%	0.01%
EB_Mem_HW	0.07%	0.06%
EM_Mem_WH	0.12%	0.01%
EB_Mem_Tx	0.12%	0.01%
D2A_HW	0.07%	0.06%
D2A_WH	0.12%	0.01%
D2A_Tx	0.12%	0.01%

6 DISCUSSION AND FUTURE WORK

This study proposes a method for evaluating the relative risk of a successful supply chain attack during the lifecycle of a CDA. As discussed, a difficulty metric based on stakeholder cybersecurity capabilities can be used to develop an overall attack risk score. Further, as demonstrated, the influence of stakeholders on attack risk can be evaluated by calculating vulnerability and recoverability scores. This information can then be used for decision-making. For instance, the acquirer or end-user may choose to require better cybersecurity via their procurement specifications from a supplier with a high vulnerability score. Alternatively, the acquirer may choose to select another supplier altogether if the vulnerable supplier has poor cybersecurity in place. Additionally, the relative supply chain attack risk can be monitored over time as security capabilities or other conditions change to provide continual awareness into supply chain cybersecurity.

To fully understand supply chain cybersecurity risk, it is necessary to gather as much information about the supply chain lifecycle, including the cybersecurity posture of all stakeholders or touchpoints involved. The modeler can use pre-existing procurement or cybersecurity maturity model questionnaires, or they can develop their own set of questions to gauge the cybersecurity capabilities at each stakeholder node. It is recommended that the end-user require third-party attestation or certification to improve answer validity. As suggested in this paper, the results can be aggregated into top-level capabilities to develop the difficulty metric. This study chose to develop a difficulty score based upon organizational, protection/prevention, and detection/response capabilities. As the questions may be highly correlated or fall into multiple capability categories, further research is needed to fully understand this effect.

Additionally, this study did not evaluate difficulty based upon specific attack scenarios or attack types (e.g., insertion, substitution, design/tool alteration, tampering, theft). Future work will evaluate the potential correlation between node, attack difficulty, and attack type as well as research other methods for acquiring and automating capability data. Furthermore, since this study assumes a CDA supply chain model is developed, consequence was not considered since operational consequence determinations are typically completed prior to procurement. As consequence also depends on component, attack type, and scenario, future work will look further into these relationships.

In addition to acquiring capability data, it is also necessary to effectively determine the capability probabilities for each stakeholder and the stakeholder impact probabilities in the leaky Noisy-MAX net CPTs for the difficulty and attack risk scores, respectively. While the baseline capability data in this study was based upon averages from [61], probability data was assigned based on expert opinion. Future research will evaluate other methodologies for determining this probability data.

7 CONCLUSIONS

Modeling the entire digital bill of materials for a supply chain is challenging given the global network of stakeholders, ubiquity of commercial off-the-shelf products, and proprietary information. As such, a BN model of a CDA's supply chain is only as good as the known information. Further, understanding the cybersecurity posture at all stakeholder nodes in a supply chain may be even more difficult to acquire. Therefore, there will always be uncertainty in the model. The key is to understand when the model is acceptable enough to provide useful information such that it can effectively drive risk reduction through security improvements at stakeholders to maintain AICE objectives throughout the product lifecycle.

This paper proposes BN analysis using the leaky Noisy-MAX parameterization to develop stakeholder difficulty and supply chain attack risk metrics using cybersecurity capability data. The difficulty metric measures how difficult it is to successfully attack a sub-component at a node in the supply chain based on the assumption that stakeholder nodes with better security will less likely be successfully attacked. The attack risk metric measures the probability of a successful attack occurring given the stakeholder difficulty scores.

Vulnerability and recoverability metrics are also proposed. Vulnerability measures the percentage of increase on attack risk on a sub-component when the stakeholder is easy to attack (State = True, NotDifficult = 100%) compared to the baseline case. Recoverability measures the percentage of decrease on attack risk when the stakeholder is very difficult to attack (State = False, Difficult = 100%) compared to the baseline case. These metrics are intended to measure the relative effects of changes for a specific supply chain, such as changes in a stakeholder's security posture or use of another supplier or distribution channel. The intent of these proposed metrics is to provide a technique for monitoring supply chain attack risk on a continual basis to provide decision-making guidance for driving risk reduction in the supply chain. Future research will continue to evaluate the effects of data selection, attack type, consequence, and technique variations to improve the model and reduce uncertainties.

8 REFERENCES

[1] Eggers, S. and K. Le Blanc, "Survey of risk analysis techniques for use in the nuclear industry," *Progress in Nuclear Energy,* Manuscript accepted for publication, 2021.

[2] ENISA, "ENISA threat landscape for supply chain attacks," European Union Agency for Cybersecurity, 2021, Available: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

[3] Heinbockel, W.J., E.R. Laderman, and G.J. Serrao, "Supply chain attacks and resiliency mitigations," The MITRE Corporation, 2017.

[4] Eggers, S. and M. Rowland, "Deconstructing the nuclear supply chain cyber-attack surface," in *Proceedings of the INMM 61st Annual Meeting*, Online Virtual Meeting, 2020: Institute of Nuclear Materials and Management.

[5] CISA, "Threat Evaluation Working Group: Supplier, products, and services threat evaluation (to include Impact Analysis and Mitigation), Version 3.0," Cybersecurity and Infrastructure Security Agency, 2021, Available: https://www.cisa.gov/publication/ict-scrm-task-force-threat-scenarios-report.

[6] NIST. *Attack surface*. National Institute of Standards and Technology. Available: https://csrc.nist.gov/glossary/term/attack_surface

[7] Eggers, S., "A novel approach for analyzing the nuclear supply chain cyber-attack surface," *Nuclear Engineering and Technology,* vol. 53, no. 3, pp. 879-887, March 2021.

[8] Windelberg, M., "Objectives for managing cyber supply chain risk," *International Journal of Critical Infrastructure Protection,* vol. 12, pp. 4-11, 2016.

[9] Wyss, G.D., J.F. Clem, J.L. Darby, K. Dunphy-Guzman, J.P. Hinton, and K.W. Mitchiner, "Risk-based cost-benefit analysis for security assessment problems," in *44th Annual 2010 IEEE International Carnahan Conference on Security Technology*, 2010, pp. 286-295: IEEE.

[10] Duran, F.A., G.D. Wyss, S.E. Jordan, and B.B. Cipiti, "Risk-Informed Management of Enterprise Security: Methodology and applications for nuclear facilities," presented at the Institute of Nuclear Materials Management 54th Annual Meeting, Palm Desert, CA, 2013.

[11] EPRI, "Cyber security technical assessment methodology, risk Informed exploit sequence identification and mitigation, Revision 1," Electric Power Research Institute, 2018.

[12] Gregorian, D. and S. Yoo, "A System-Theoretic Approach to Risk Analysis," M.S., Engineering and Management, Massachusetts Institute of Technology, 2021.

[13] NRC, "NUREG/CR-6847 Cyber security self-assessment method for U.S. nuclear power plants," U.S. Nuclear Regulatory Commission, Washington D. C., 2004.

[14] Knowles, W., D. Prince, D. Hutchison, J.F.P. Disso, and K. Jones, "A survey of cyber security management in industrial control systems," *International Journal of Critical Infrastructure Protection,* vol. 9, pp. 52-80, 2015.

[15] Voronca, S. and S. Voronca, "Survey of existing risk assessment and management standards applied worldwide, for power companies," in *6th International Conference on Modern Power Systems*, Cluj-Napoca, Romania, 2015, pp. 369-373.

[16] Kriaa, S., L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand, "A survey of approaches combining safety and security for industrial control systems," *Reliability Engineering & System Safety,* vol. 139, pp. 156-178, 2015.

[17] Nissen, C., J. Gronager, R. Metzger, and H. Rishikof, "Deliver uncompromised: A strategy for supply chain security and resilience in response to the changing character of war," The MITRE Corporation, 2019.

[18] SAE, "SAE AS5553C, Counterfeit Electrical, Electronic, and Electromechanical (EEE) parts; Avoidance, detection, mitigation, and disposition," SAE International, 2019.

[19] SAE, "SAE AS6081, Fraudulent/counterfeit electronic parts: Avoidance, detection, mitigation, and disposition - distributors," SAE International, 2012.

[20] SAE, "SAE ARP9134A, Supply chain risk management guideline," SAE International, 2014.

[21] *DoDI 5000.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN), Incorporating Change 3,* DoD CIO/USD(R&E), 2018.

[22] *Defense Acquisition Guidebook, Chapter 9, Rev 5: Program Protection*. Defense Acquisition University, 2017.

[23] *48 CFR § 252.246-7007 Contractor Counterfeit Electronic Part Detection and Avoidance System*, 2021.

[24] *48 CFR § 252.246-7008 - Sources of Electronic Parts*, 2021.

[25] *DoDI 5000.02 Operation of the Defense Acquisition System, Incorporating Change 3,* USD(AT&L), 2017.

[26] *DoDI 5000.47E, Anti-Tamper (AT), Incorporating Change 3,* USD(A&S), 2018.

[27] DOD, "Cybersecurity Maturity Model Certification (CMMC), Version 1.02," Department of Defense, 2020.

[28] DOE, "Cybersecurity Capability Maturity Model (C2M2) Version 2," Department of Energy, 2019.

[29] EPRI, "Cyber security procurement methodology for power delivery systems," Electric Power Research Institute, 2012.

[30] ESCSWG, "Cybersecurity procurement language for energy delivery systems," Energy Sector Control Systems Working Group, 2014, Available: https://www.energy.gov/sites/default/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf.

[31] NERC, "CIP-013-1, Cyber security - Supply chain risk management," North American Electric Reliability Council, 2018.

[32] EPRI, "Cyber Security in the supply chain: Cyber security procurement methodology, Revision 2," Electric Power Research Institute, 2018.

[33] EPRI, "Secure development, integration, and delivery (SDID) audit topical guide," Electric Power Research Institute, 3002015793, 2019, Available: https://www.epri.com/research/products/000000003002015793.

[34] NEI, "Addendum 3 to NEI 08-09, Cyber security plan for nuclear power reactors, Revision 6, Systems and Services Acquisition," Nuclear Energy Institute, August 2017.

[35] DHS, "Department of Homeland Security: Cyber Security Procurement Language for Control Systems," Department of Homeland Security, September 2009.

[36] IEC, "IEC 62443-2-4, Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers," International Electrotechnical Commission, 2017.

[37] IEC, "IEC 62443-4-1, Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements," International Electrotechnical Commission, September, 2016 2017.

[38] UL, "UL 2900-2-2, Outline of investigation for software cybersecurity for network-connectable products, Part 2-2: Particular requirements for industrial control systems, Edition 1," 2017.

[39] CISA, "Vendor supply chain risk managment (SCRM) template," Cybersecurity and Infrastructure Security Agency, 2021, Available: https://www.cisa.gov/publication/ict-scrm-task-force-vendor-template.

[40] CISA, "Mitigating ICT supply chain risks with qualified bidder and manufacturer lists," Cybersecurity and Infrastructure Security Agency, 2021, Available: https://www.cisa.gov/publication/ict-scrm-task-force-qualified-lists-report.

[41] ISO/IEC, "ISO/IEC 27036-3:2013, Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security," International Organization for Standardization/International Electrotechnical Commission, 2013.

[42] ISO/IEC, "ISO/IEC 20243-1:2018, Information technology — Open Trusted Technology ProviderTM Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products — Part 1: Requirements and recommendations," International Organization for Standardization/International Electrotechnical Commission, 2018.

[43] Boyens, J., C. Paulsen, N. Bartol, R. Moorthy, and S.A. Shankles, "NISTIR 7622: Notional supply Chain risk management practices for federal information systems," *National Institute of Standards and Technology, Maryland,* pp. 1-3, 2012.

[44] Stouffer, K., V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "SP 800-82, Revision 2: Guide to industrial control systems (ICS) security," National Institute of Standards and Technology, 2015.

[45] NIST, "SP 800-147, BIOS protection guideline," National Institute of Standards and Technology, 2011.

[46] NIST, "SP 800-147b, BIOS protection guidelines for servers," National Institute of Standards and Technology, 2014.

[47] Boyens, J., C. Paulsen, R. Moorthy, N. Bartol, and S.A. Shankles, "NIST Special Publication 800-161 Supply chain risk management practices for federal information systems and organizations," 2015.

[48] UL, "UL 2900-1, Standard for software cybersecurity for network-connectable products, Part 1: General requirements, Edition 1," 2017.

[49] SAFECode, "Fundamental practices for secure software development, Third Edition," Software Assurance Forum for Excellence in Code, 2018, Available: https://safecode.org/wp-content/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf.

[50] SAFECode, "Framework for supply chain integrity," Software Assurance Forum for Excellence in Code, 2014, Available: http://safecode.org/wp-content/uploads/2014/06/SAFECode_Supply_Chain0709.pdf.

[51] SAFECode, "Managing security risks inherent in the use of third-party components," Software Assurance Forum for Excellence in Code, 2019, Available: https://www.safecode.org/wp-content/uploads/2017/05/SAFECode_TPC_Whitepaper.pdf.

[52] CISA, "Defending against software supply chain attacks," Cybersecurity and Infrastructure Security Agency, 2021, Available: https://www.cisa.gov/publication/software-supply-chain-attacks.

[53] Pai, R.R., V.R. Kallepalli, R.J. Caudill, and M. Zhou, "Methods toward supply chain risk analysis," in *SMC'03 Conference Proceedings. 2003 IEEE International Conference on Systems, Man and Cybernetics. Conference Theme-System Security and Assurance (Cat. No. 03CH37483)*, 2003, vol. 5, pp. 4560-4565: IEEE.

[54] Hosseini, S. and K. Barker, "Modeling infrastructure resilience using Bayesian networks: A case study of inland waterway ports," *Computers & Industrial Engineering,* vol. 93, pp. 252-266, 2016.

[55] Barker, K., J.E. Ramirez-Marquez, and S. Hosseini, "Improved Acquisition for System Sustainment: Resilient Supplier Evaluation and Selection with Bayesian Networks," Acquisition Research Program, 2018.

[56] Hosseini, S. and K. Barker, "A Bayesian network model for resilience-based supplier selection," *International Journal of Production Economics,* vol. 180, pp. 68-87, 2016.

[57] Woudenberg, S.P. and L.C. Van Der Gaag, "Using the noisy-OR model can be harmful… but it often is not," in *European Conference on Symbolic and Quantitative Approaches to Reasoning and Uncertainty*, 2011, pp. 122-133: Springer.

[58] Fenton, N.E., T. Noguchi, and M. Neil, "An extension to the noisy-OR function to resolve the 'explaining away'deficiency for practical Bayesian network problems," *IEEE transactions on knowledge and data engineering,* vol. 31, no. 12, pp. 2441-2445, 2019.

[59] Dıez, F.J. and M.J. Druzdzel, "Canonical Probabilistic Models for Knowledge Engineering."

[60] Diez, F.J., "Parameter adjustment in Bayes networks. The generalized noisy OR–gate," in *Uncertainty in artificial intelligence*, 1993, pp. 99-105: Elsevier.

[61] IPA, "Information Security Measures Benchmark, Ver. 5.0," Information Technology Protection Agency, Japan, 2020, Available: https://security-shien.ipa.go.jp/manual/Ver.5.0%E8%A8%BA%E6%96%AD%E3%83%87%E3%83%BC%E3%82%BF%E7%B5%B1%E8%A8%88%E6%83%85%E5%A0%B1.pdf.

Annex A:
CISA Vendor Supply Chain Risk Management (SCRM) Template [39]

VENDOR SUPPLY CHAIN RISK MANAGEMENT (SCRM) TEMPLATE

April 2021

This page is intentionally left blank.

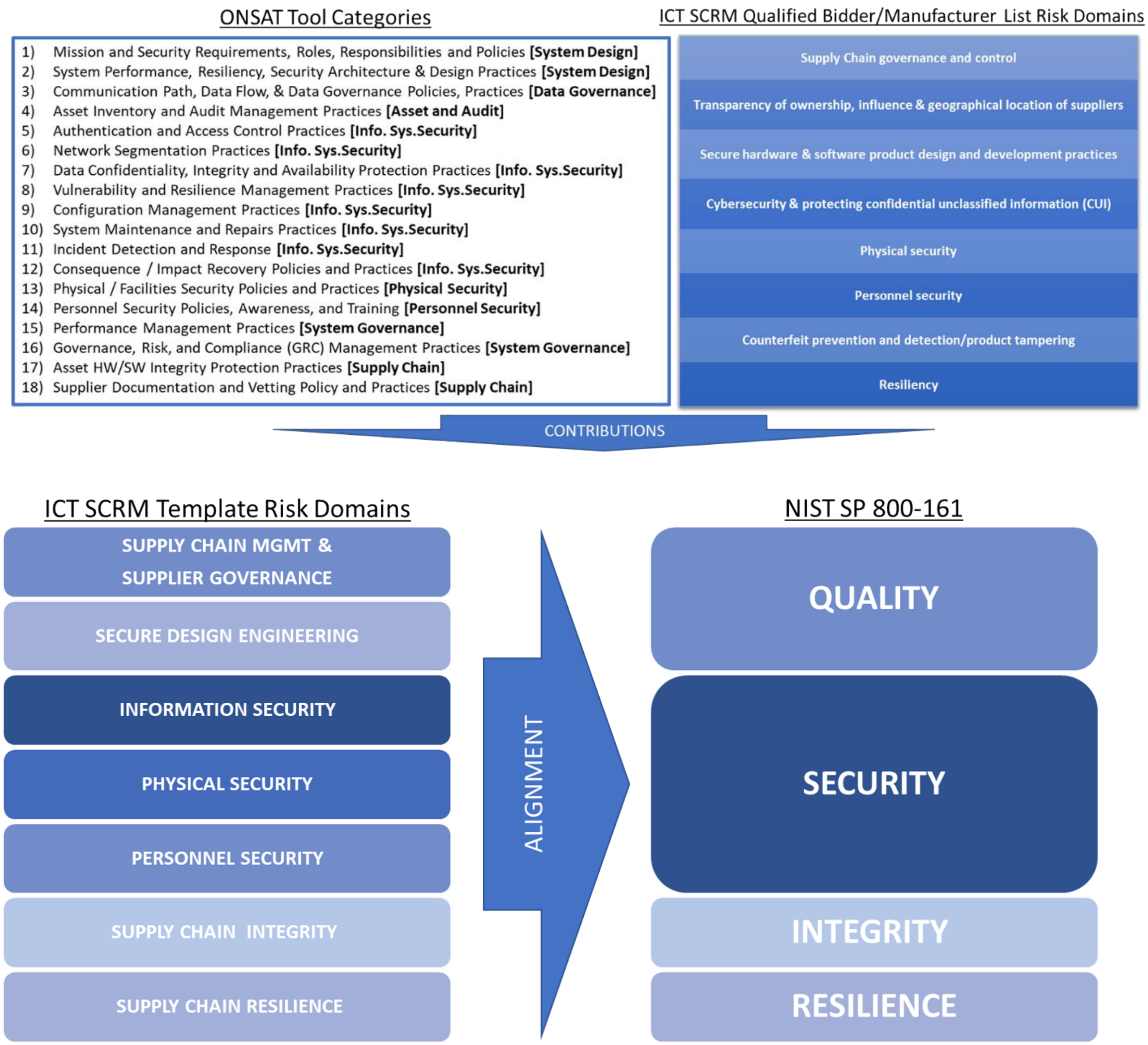
VENDOR SUPPLY CHAIN RISK MANAGEMENT (SCRM) TEMPLATE

Abstract

The following document is the result of a collaborative effort produced by the Cybersecurity and Infrastructure Security Agency (CISA) Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force, Working Group 4 (hereinafter WG4), aimed at creating a standardized template of questions as a means to communicate ICT supply chain risk posture in a consistent way among public and private organizations of all sizes. The purpose of this assessment template is to normalize a set of questions regarding an ICT Supplier/Provider implementation and application of industry standards and best practices. This will enable both vendors and customers to communicate in a way that is more consistently understood, predictable, and actionable. These questions provide enhanced visibility and transparency into entity trust and assurance practices and assist in informed decision-making about acceptable risk exposure.

This assessment may be used to illuminate potential gaps in risk management practices and provides a flexible template that can help guide supply chain risk planning in a standard way. It is meant to be non-prescriptive and no specific use case is being mandated. The suggested use is as a tool for consistently analyzing risk when comparing potential new providers. This template builds upon existing industry standards to provide step-by-step guidance and improved awareness Key categories of vendor SCRM compliance are defined within the document, building on a framework of established industry standards and other Task Force efforts, while incorporating inputs from key industry standards and best practices, such as NIST SP 800-161, the Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC), and the Outsourcing Network Services Assessment Tool (ONSAT).

The graphics below illustrate the incorporation of ONSAT Tool categories and input from the ICT SCRM Qualified Bidder/Manufacturer Lists (from CISA ICT SCRM Task Force Working Group 3) across the Template categories, as well as alignment of the Template categories to the NIST SP 800-161 categories.



ONSAT Tool Categories

1) Mission and Security Requirements, Roles, Responsibilities and Policies **[System Design]**
2) System Performance, Resiliency, Security Architecture & Design Practices **[System Design]**
3) Communication Path, Data Flow, & Data Governance Policies, Practices **[Data Governance]**
4) Asset Inventory and Audit Management Practices **[Asset and Audit]**
5) Authentication and Access Control Practices **[Info. Sys.Security]**
6) Network Segmentation Practices **[Info. Sys.Security]**
7) Data Confidentiality, Integrity and Availability Protection Practices **[Info. Sys.Security]**
8) Vulnerability and Resilience Management Practices **[Info. Sys.Security]**
9) Configuration Management Practices **[Info. Sys.Security]**
10) System Maintenance and Repairs Practices **[Info. Sys.Security]**
11) Incident Detection and Response **[Info. Sys.Security]**
12) Consequence / Impact Recovery Policies and Practices **[Info. Sys.Security]**
13) Physical / Facilities Security Policies and Practices **[Physical Security]**
14) Personnel Security Policies, Awareness, and Training **[Personnel Security]**
15) Performance Management Practices **[System Governance]**
16) Governance, Risk, and Compliance (GRC) Management Practices **[System Governance]**
17) Asset HW/SW Integrity Protection Practices **[Supply Chain]**
18) Supplier Documentation and Vetting Policy and Practices **[Supply Chain]**

ICT SCRM Qualified Bidder/Manufacturer List Risk Domains

Supply Chain governance and control

Transparency of ownership, influence & geographical location of suppliers

Secure hardware & software product design and development practices

Cybersecurity & protecting confidential unclassified information (CUI)

Physical security

Personnel security

Counterfeit prevention and detection/product tampering

Resiliency

ICT SCRM Template Risk Domains

SUPPLY CHAIN MGMT & SUPPLIER GOVERNANCE

SECURE DESIGN ENGINEERING

INFORMATION SECURITY

PHYSICAL SECURITY

PERSONNEL SECURITY

SUPPLY CHAIN INTEGRITY

SUPPLY CHAIN RESILIENCE

NIST SP 800-161

QUALITY

SECURITY

INTEGRITY

RESILIENCE

Contents

INTRODUCTION

The questions below broadly cover ICT Supply Chain Risk Management, governance, and associated risk domains. The intent is to illuminate the risk factors that the acquiring organization requires to understand how the risk profile of the entity aligns with their tolerance of risk for the specific product/service being provided. They will aid in mitigating (not eliminating) risk and are consistent with commercial and public sector standards. The questions should be used as applicable, depending on the product/service and the customer involved (*e.g.,* DoD, civilian, commercial).

Recommended Use

- Provide a contact (name, email, and phone number) for questions, support, or additional information related to the questionnaire to the respondents.
- Please provide a response to each 'Yes', 'No' question as relevant to the offering.
- If the question does not apply to your organization, please answer 'N/A' and provide a supporting statement of applicability if not relevant to the offering in consideration.
- A response of 'Alternate' may be used if a particular supply chain risk can be addressed in alternative ways and not directly through compliance with a standard or framework.
- Please attach supporting documents to the completed questionnaire. You may provide links when submitting if documentation is available online and accessible.
- If the respondent(s) is able provide proof of affirmative answers to the initial "bypass questions", the remainder of the assessment is not required.

We recommend designating one primary POC from your organization who will collaborate with the appropriate POCs/teams/vendor/supplier to coordinate and collect and compile responses for each section. The appropriate POCs within each organization will vary and may consist of individuals in acquisition, procurement, supply chain, or security offices. While related, each section is design to be relevant to a different aspect of your organization.

This template is intended to gather an initial and consistent baseline and additional follow-up questions from the organization, or other documentation, may be warranted.

1. QUALIFYING QUESTIONS

If you can provide affirmative responses to the questions below AND supporting, non-expired documentation, you may skip ALL remaining questions.

1.1. Have you previously provided supply chain risk management information to this organization?

If 'Yes,' please provide an updated revision covering material changes.

OR

1.2. Do you have controls fully aligned to NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organization?

1.2.1. Please provide proof of the scope of controls implemented and how controls were validated.

1.2.2. Provide any additional supporting documentation of relevant and current third-party assessments or certification for supply chain risk management, such as ANSI/ASIS SCRM 1.2014, ISO 28000:2007, ISO 31000, ISO 20243, etc.

If you responded affirmatively to ANY of the questions above, you may attach supporting documentation, **skip the remaining questions,** and continue to the signature page.

2. SUPPLY CHAIN MANAGEMENT AND SUPPLIER GOVERNANCE

General

2.1. Do you have policies to ensure timely notification of updated risk management information previously provided to us?

[Yes, No, Alternate, or N/A]

2.1.1. How do you notify us of changes?

2.1.2. What is your customer notification policy?

Information Communications Technology (ICT) Supply Chain Management

2.2. Do you have a documented Quality Management System (QMS) for your ICT supply chain operation based on an industry standard or framework?

[Yes, No, Alternate, or N/A]

2.2.1. Please provide the document which describes your QMS, including any standards or frameworks to which it is aligned.

2.3. Do you have an organization-wide strategy for managing end-to-end supply chain risks (from development, acquisition, life cycle support, and disposal of systems, system components, and to system services)?

[Yes, No, Alternate, or N/A]

2.3.1. What is your strategy?

2.3.2. How have you implemented it?

Authentication and Provenance

2.4. Do you have a policy or process to ensure that none of your suppliers or third-party components are on any banned list?

[Yes, No, Alternate, or N/A]

2.5. Do you provide a bill of materials (BOM) for your products, services, and components which includes all logic-bearing (e.g., readable/writable/programmable) hardware, firmware, and software?

[Yes, No, Alternate, or N/A]

2.5.1. If you provide a BOM that does not include all logic-bearing hardware, firmware, and software, what does your BOM include?

2.5.2. Upon request, are you able to provide your BOM including all logic-bearing hardware, firmware, and software?

2.5.3. How do you track changes in your products, services, and components and how do you reflect those changes in the applicable BOM(s)?

2.6. For hardware components included in the product offering, do you only buy from original equipment manufacturers or licensed resellers?

[Yes, No, Alternate, or N/A]

2.7. Do you have a process for tracking and tracing your product while in development and manufacturing?

[Yes, No, Alternate, or N/A]

2.7.1. How do you keep track of your chain of custody?

2.7.2. How do you track and trace components within your product?

Supplier Governance

2.8. Do you have written Supply Chain Risk Management (SCRM) requirements in your contracts with your suppliers?

[Yes, No, Alternate, or N/A]

2.8.1. What are your SCRM requirements?

2.8.2. How do you verify that your suppliers are meeting contractual terms and conditions, which may include requirements to be passed down to sub-suppliers?

2.8.3. If violations of contractual SCRM requirements or SCRM-related incidents occur, do you ensure and monitor any remediation activities?

2.9. Do you revise your written SCRM requirements regularly to include needed provisions?

2.10. Do you have policies for your suppliers to notify you when there are changes to their subcontractors or their offerings (components, products, services, or support activities)?

[Yes, No, Alternate, or N/A]

2.10.1. Please describe your policy.

3. SECURE DESIGN AND ENGINEERING

Note: If your answer to the question below is 'Yes,' please continue and complete the remaining questions in this section. If your answer is 'No,' you may skip the remainder of this section and move on to the next section of this questionnaire.

3.1. Does your organization develop (or integrate) custom hardware or software offerings?

[Yes, No, Alternative]

3.1.1. List the custom software, hardware, system, or solution offering(s) provided by your organization.

Product Offering Lifecycle Management and Organization

3.2. Do you implement formal organizational roles and governance responsible for the implementation and oversight of Secure Engineering across the development or manufacturing process for product offerings?

[Yes, No, Alternate, or N/A]

3.2.1. If so, how are roles, responsibilities, and practices validated?

3.3. What security control framework (industry or customized) is used to define product offering security capabilities?

Please describe or 'N/A'

3.4. Does your organization document and communicate security control requirements for your hardware, software, or solution offering?

[Yes, No, Alternate, or N/A]

3.4.1. How are security requirements validated as part of the product offering development or manufacturing process?

3.5. How does your organization implement development and manufacturing automation to enforce lifecycle processes and practices?

Protect IP and Product (Supplier) Offering Assets

3.6. Does your organization protect all forms of code from unauthorized access and tampering, including patch updates?

[Yes, No, Alternate, or N/A]

3.6.1. How does your organization prevent unauthorized changes to code, both inadvertent and intentional, which could circumvent or negate the intended security characteristics of the software?

3.7. Does your organization provide a mechanism for verifying software release integrity, including patch updates for your software product offering?

[Yes, No, Alternate, or N/A]

3.8. How does your organization prevent malicious and/or counterfeit IP components within your product offering or solution?

3.9. Does your organization manage the integrity of IP for its product offering?

[Yes, No, Alternate, or N/A]

3.9.1. How does your organization archive assets associated with the product offering development or manufacturing process?

Secure Coding and Manufacturing Practices

3.10. Does your organization define, follow, and validate secure coding and manufacturing practices to mitigate security risks?

[Yes, No, Alternate, or N/A]

3.10.1. How does your organization conduct threat modeling to determine required product offering security requirements?

3.10.2. How does your organization determine how identified risks are mitigated in product offering design?

3.10.3. How does your organization justify risk-based decisions to relax or waive security requirements or controls?

3.10.4. How does your organization validate that the offering will meet the security requirements and satisfactorily address the identified threat assessment?

3.11. Does your organization verify that third-party software provides required security requirements/controls?

[Yes, No, Alternate, or N/A]

3.11.1. How does your organization reduce the risk associated with using acquired software modules and services, which are potential sources of additional vulnerabilities?

3.12. Does your organization reuse existing, well-secured software and hardware components, when feasible, instead of duplicating functionality?

[Yes, No, Alternate, or N/A]

3.13. Does your organization configure the compilation and build processes to improve executable security?

[Yes, No, Alternate, or N/A]

3.13.1. How does your organization decrease the number of security vulnerabilities in the software and reduce costs by eliminating vulnerabilities before testing occurs?

3.14. Does your organization implement formal vulnerability and weakness analysis practices?

[Yes, No, Alternate, or N/A]

3.14.1. Does your organization automate the identification of security vulnerabilities and weaknesses?

3.14.2. Does your organization test executable code or components to identify vulnerabilities and verify compliance with security requirements?

3.15. Does your organization configure offerings to implement secure settings by default?

[Yes, No, Alternate, or N/A]

3.15.1. Does your organization test offerings using hardened runtime environments?

Respond to Vulnerabilities (RV)

3.16. Does your organization maintain and manage a Product Security Incident Reporting and Response program (PSRT)?

[Yes, No, Alternate, or N/A]

3.16.1. How does your organization assess, prioritize, and remediate reported vulnerabilities?

3.16.2. How does your organization ensure that vulnerabilities are remediated in a timely period, reducing the window of opportunity for attackers?

3.17. Does your organization analyze vulnerabilities to identify root cause?

[Yes, No, Alternate, or N/A]

3.17.1. Are vulnerability root causes used as input to update secure development process, tools, and training to lower future vulnerabilities?

4. INFORMATION SECURITY

4.1. Do you hold a valid information security/cybersecurity third-party attestation or certification? (e.g., ISO 27001, SOC 2 Type 2, CMMC Level 3-5, Cybersecurity Maturity Assessment, etc.)

[If yes, please state the program and date that you were certified, and provide a copy of the certification. You may skip the remaining questions of this section and proceed to the following section. If no, continue.]

4.2. Do you follow operational standards or frameworks for managing Information Security/Cyber security? (e.g., NIST CSF 1.1, NIST 800-37, Rev. 2, NIST SP 800-161, ISO IEC 27001, ISO 20243, ISO 27036, SAE AS649)

[Yes, No, Alternate, or N/A]

4.2.1. If so, please state which one(s)?

4.3. Do you have company-wide, publicly available information security policies in place covering privacy policies?

[Yes, No, Alternate, or N/A]

4.3.1. If 'Yes', please provide.

4.3.2. What mechanisms are in place to ensure your policies are enforced within your supply chain?

4.3.2.1. Do you receive notification of and have a response plan in place for privacy violations of the suppliers in your supply chain?

Asset Management

4.4. Do you inventory and audit back-up and/or replacement hardware and software assets to ensure their accountability and integrity?

[Yes, No, Alternate, or N/A]

4.4.1. What recognized standards or frameworks do you follow to ensure integrity of back-up assets? (e.g., NIST 800-53, NIST 800- 171 DFARS, ISA/IEC 62443 or ISO 27001/2)

4.5. Do you have a defined governance scope for asset management, including line of business technology, facilities, devices, and all other data- generating hardware (like Internet of Things devices)?

[Yes, No, Alternate, or N/A]

4.6. Do you have processes or procedures in place to ensure that devices and software installed by users external to your IT department (e.g., line of business personnel) are being discovered, properly secured, and managed?

[Yes, No, Alternate, or N/A]

4.6.1. What, if any, types of assets are out of scope for your tracking procedures?

4.7. Do you have an asset management program approved by management for your IT assets that is regularly maintained?

[Yes, No, Alternate, or N/A]

4.7.1. What are your methods to manage IT assets on the network?

4.7.1.1. How do you manage other IT hardware and software assets which are not network connected, regardless of network presence?

4.7.2. What are your methods of verifying acceptable use of assets, including verified asset return, for your network-connected assets?

4.8. Do you have documented policies or procedures to manage enterprise network-connectable assets throughout their lifecycle?

[Yes, No, Alternate, or N/A]

4.8.1. What are your processes to manage obsolescence of network-connected assets?

4.8.2. What are your policies or procedures to ensure your enterprise software platforms and applications, and hardware assets, are classified according to their criticality?

4.8.3. What are your policies or procedures to ensure appropriate controls are in place for internal or third-party cloud services?

4.9. Do you ensure that you are not sourcing assets on a banned list to customers (e.g., ITAR, NDAA Section 889)?

[Yes, No, Alternate, or N/A]

4.9.1. How do you ensure that you are not providing assets on a banned list to customers?

4.10. Do you have documented hardware and software policies and practices in place to ensure asset integrity?

[Yes, No, Alternate, or N/A]

4.10.1. What recognized standards or frameworks are followed to ensure asset integrity?

4.10.1.1. How do you ensure that regular reviews and updates of the asset integrity policies and practices are performed?

Identify

4.11. Do you have documented policies or procedures for identification and detection of cyber threats?

[Yes, No, Alternate, or N/A]

4.11.1. What processes do you have in place to promptly detect cyber threats?

4.11.1.1. How do you manage the identification of threats within your supply chain, including suppliers and sub-contractors?

4.11.1.2. What processes are in place to act upon external credible cyber security threat information received?

4.12. Do you address the interaction of cybersecurity operational elements (e.g., SOC, CSIRT, etc.) with the physical security operational elements protecting the organization’s physical assets?

[Yes, No, Alternate, or N/A]

4.12.1. How do you ensure that physical security incidents and suspicious events are escalated to cybersecurity operations staff?

4.12.2. Are cybersecurity vulnerabilities for industrial control systems, including physical access controls and video monitoring systems, tracked?

4.12.3. What standards or frameworks are followed for management of IT and OT system interactions?

4.13. Do you have a policy or procedure for the handling of information that is consistent with its classification?

[Yes, No, Alternate, or N/A]

4.13.1. What is your process to verify that information is classified according to legal, regulatory, or internal sensitivity requirements?

4.13.1.1. How do you convey requirements for data retention, destruction, and encryption to your suppliers?

4.14. Do you have documented policies or procedures for internal identification and management of vulnerabilities within your networks and enterprise systems?

[Yes, No, Alternate, or N/A]

4.14.1. What industry standards or frameworks are followed for vulnerability management

4.14.1.1. How do you identify vulnerabilities in your supply chain (suppliers/sub-contractors) before they pose a risk to your organization?

4.14.1.2. How do you assess and prioritize the mitigation of vulnerabilities discovered on your internal networks and systems? (e.g., asset criticality, exploitability, severity, etc.)

Protect

4.15. Do you have network access control policies and procedures in place for your information systems that are aligned with industry standards or control frameworks?

[Yes, No, Alternate, or N/A]

4.15.1. If Yes, please list any standards or frameworks used.

4.15.2. What are your practices for items such as federation, privileged users, and role-based access control for end-user devices?

4.15.2.1. How do you ensure remote access is managed for end-user devices or employees and suppliers, including deactivation of accounts? (e.g. Multi-factor authorization, encryption, protection from malware, etc.)

4.15.2.2. How do you identify and correct end-user systems that fall out of compliance?

4.16. Is cybersecurity training required for personnel who have administrative rights to your enterprise computing resources?

[Yes, No, Alternate, or N/A]

4.16.1. What is the frequency for verifying personnel training compliance?

4.16.2. What cybersecurity training is required for your third-party stakeholders (e.g., suppliers, customers, partners, etc.) who have network access?

4.16.2.1. How is training compliance tracked for third parties with network access?

4.17. Do you include contractual obligations to protect information and information systems handled by your suppliers?

[Yes, No, Alternate, or N/A]

4.17.1. What standard cybersecurity standards or frameworks are the contractual supplier terms for information protection aligned to, if any?

4.18. Do you have an organizational policy on the use of encryption that conforms with industry standards or control frameworks?

[Yes, No, Alternate, or N/A]

4.18.1. What industry standards or controls frameworks are followed for encryption and key management?

4.18.2. What processes or procedures exist to comprehensively manage the use of encryption keys?

4.18.2.1. What is your process for protecting data at rest and in transit?

4.19. Does your organization have hardening standards in place for network devices (e.g., wireless access points, firewalls, etc.)?

[Yes, No, Alternate, or N/A]

4.19.1. What protections exist to provide network segregation where appropriate (e.g., intrusion detection systems)?

4.19.2. What controls exist to continuously monitor changes to your network architecture (e.g., NIST 800-53 or related controls)?

4.19.3. How do you manage prioritization and mitigation of threats discovered on your networks?

4.19.4. How do you track changes to software versions on your servers?

4.20. Do you follow an industry standard or framework for your internal or third- party cloud deployments, if applicable?

[Yes, No, Alternate, or N/A]

4.20.1. What protections are in place between your network and cloud service providers?

4.20.1.1. How to do you convey cloud security requirements to your suppliers/sub-contractors?

Detect

4.21. Do you have defined and documented incident detection practices that outline which actions should be taken in the case of an information security or cybersecurity event?

[Yes, No, Alternate, or N/A]

4.21.1. Are cybersecurity events centrally logged, tracked, and continuously monitored?

4.21.2. Are incident detection practices continuously improved?

4.22. Do you require vulnerability scanning of software running within your enterprise prior to acceptance?

[Yes, No, Alternate, or N/A]

4.22.1. What procedures or policies exist, if any, for detecting vulnerabilities in externally obtained software (such as penetration testing of enterprise and non-enterprise software)?

4.22.2. What are your procedures to scan for vulnerabilities in supplier-provided software running on your network?

4.23. Do you manage updates, version tracking of new releases, and patches (including patching history) for your software and software services offerings?

[Yes, No, Alternate, or N/A]

4.23.1. What is the responsibility of the product end-user (customer) for updating software versions?

4.24. Do you deploy anti-malware software?

[Yes, No, Alternate, or N/A]

4.24.1. What systems are out of scope for anti-malware software compliance, if any?

4.24.1.1. How do you ensure anti-malware is present on developer platforms? As applicable to your offering?

Respond & Recover

4.25. Do you have a documented incident response process and a dedicated incident response team (CSIRT - Computer Security Incident Response Team)?

[Yes, No, Alternate, or N/A]

4.25.1. What is your process for reviewing and exercising your resiliency plan?

4.25.2. What is your process to ensure customers and external entities (such as government agencies) are notified of an incident when their product or service is impacted?

4.26. Do you have processes or procedures to recover full functionality, including integrity verification, following a major cybersecurity incident?

[Yes, No, Alternate, or N/A]

4.26.1. What is the frequency for testing of back-up media?

4.27. Do you insure for financial harm from a major cybersecurity incident (e.g., self-insure, third-party, parent company, etc.)?

[Yes, No, Alternate, or N/A]

4.27.1. Does coverage include financial harm to your customers resulting from a cybersecurity breach which has impacted your company?

5. PHYSICAL SECURITY

5.1. Is the entity (organization, operational unit, facility, etc.) currently covered by an unrestricted/unlimited National Industrial Security Program (NISP) Facility Clearance (FCL) or a related U.S. government program such as C- TPAT that certifies the entity as meeting appropriate physical security standards?

[If 'Yes,' please state the program that certified you and date of last certification. You may skip the remaining questions of this section and proceed to the next section. If not, continue with this section.]

5.1.1. If the entity is not covered by a NISP FCL but currently has some other US Government or industry attestation, such as TAPA FSR of meeting a physical security code or standard, please identify the standard, the issuing agency, and the most recent date of certification.

5.1.2. Is the entity covered by a limited FCL (in agreement with a foreign government)? Describe.

5.2. Do you have documented security policies and procedures that address the control of physical access to cyber assets (network devices, data facilities, patch panels, industrial control systems, programmable logic, etc.)?

[Yes, No, Alternate, or N/A]

5.2.1. To what standards/controls do you adhere? (e.g., NIST publication, ISO, UL, etc.)

5.2.1.1. How often do you review and update to those policies and procedures and what is the most recent review?

5.2.1.2. If needed, can you provide these documents for our review?

5.3. Do you have documented policies addressing staff training which includes procedures to limit physical access to cyber assets to only those with demonstrated need?

[Yes, No, Alternate, or N/A]

5.3.1. What training do all staff receive to address potential physical security threats and how to respond to emergencies (e.g., fire, weather, etc.)?

5.3.2. What training do cybersecurity staff, physical security staff, and contractors with at least limited access to sensitive areas of a facility receive?

5.3.2.1. How does this training address potential threats to the facility and how the physical access controls are integrated with system network interfaces?

5.3.3. What standards do you follow, or did you implement (e.g., NIST publication, ISO, UL, etc.)?

5.3.3.1. How is this training documented?

5.4. Do you have a documented Security Incident Response process covering physical security incidents? (e.g., potential intruder access, missing equipment, etc.)

[Yes, No, Alternate, or N/A]

5.4.1. What processes do you have in place to document the actions taken during and after an actual or suspected physical security incidents (e.g., security log, formal report to management, police report, etc.)?

5.4.1.1. How do you ensure that your staff understands and complies with procedures (e.g., training, exercises, and actual cases of incident response)?

5.5. For facilities that use an independent contractor for physical security, are physical facilities security policy and procedures incorporated into service level agreements, contracts, policies, regulatory practices?

[Yes, No, Alternate, or N/A]

5.5.1. What physical / facilities security policies and practices are subject to audit?

5.5.2. For contractors who have access to a critical facility, sensitive assets, or major physical plant systems, what standards are they required to attest to? (e.g., NIST publication, ISO, UL, etc.)

5.5.2.1. How is compliance with these standards validated?

5.6. Are there enforcement mechanisms (e.g., sanctions, response procedures, technology) for unauthorized physical access to mission/business critical information, functions, services and assets?

[Yes, No, Alternate, or N/A]

5.6.1. What type of action or response would be taken for unauthorized physical access to sensitive cyber assets?

5.7. Do you have evidence that physical security mechanisms are effective and adequate to protect assets? Evidence could include third-party assessment, self-assessment, records of actions taken to enforce rules, etc.

[Yes, No, Alternate, or N/A]

5.7.1. What is the date of the last review and update to your enforcement strategy?

Physical Security In-transit

5.8. Do you utilize a controlled bill of materials (BOM) or similar capability to protect assets that are being received, in process, or in-transit?

[Yes, No, Alternate, or N/A]

5.8.1. What industry standards or frameworks are followed?

5.9. Do you have requirements that all items being shipped have tamper-evident packaging?

[Yes, No, Alternate, or N/A]

5.9.1. What industry standards or frameworks are being followed to ensure packaging is tamper-evident?

5.9.1.1. How are these requirements audited to ensure that they are effective?

5.10. Do you have processes in place to prevent counterfeit parts from entering your supply chain?

[Yes, No, Alternate, or N/A]

5.10.1. What requirements, if any, are in place to ensure the use of Original Equipment Manufacturer (OEM) or Authorized Distributors for all key components?

5.10.2. What are your processes for the detection and disposition of counterfeit electronic components?

5.10.2.1. How do you pass on counterfeit prevention requirements to your third-party suppliers?

6. PERSONNEL SECURITY

6.1. Does a formal personnel security program exist?

[Yes, No, Alternate, or N/A]

6.1.1. Is employee access managed by role?

6.1.2. Is access to business-critical systems, manufacturing facilities, and assets formally managed and maintained? Please describe.

6.1.3. Are physical security practices formally governed, documented, maintained, and enforced?

Onboarding

6.2. Do you have a process for onboarding personnel?

[Yes, No, Alternate, or N/A]

6.2.1. Does the process include security awareness training?

6.2.2. What is the process to determine the level of access to company identifications (IDs), tokens, documents, applications, etc.?

6.2.3. What is the process to distribute company assets?

6.2.4. Is the onboarding process documented?

6.2.4.1. If ‘Yes’, please provide a copy.

6.3. Do you have policies for conducting background checks of your employees as permitted by the country in which you operate?

[Yes, No, Alternate, or N/A]

6.3.1. If not permitted by the country, please note that and provide the part of your supply chain for which it is applicable.

6.3.2. How do you conduct the background checks and document, validate, and update their responses?

6.4. Do you have policies for conducting background checks for your suppliers, as permitted by the country in which you operate?

[Yes, No, Alternate, or N/A]

6.4.1. If not permitted by the country, please note that and provide the part of your supply chain for which it is applicable.

6.4.2. How do you conduct the background checks and document, validate, and update their responses?

6.5. Do you have policies for conducting background checks for any subcontractors, as permitted by the country in which you operate?

[Yes, No, Alternate, or N/A]

6.5.1. If not permitted by the country, please note that and provide the part of your supply chain for which it is applicable.

6.5.2. How do you conduct the background checks and document, validate, and update their responses?

Offboarding

6.6. Do you have a process for offboarding personnel?

[Yes, No, Alternate, or N/A]

6.6.1. Does the process include a process to transfer knowledge to other personnel?

6.6.2. What is the process to remove access to all company documents, applications, assets, etc.?

6.6.3. What is the process to recover all company assets?

6.6.4. Is that process documented?

Awareness and Training (Security-Specific)

6.7. Are personnel security practices formally documented and accessible to all employees?

[Yes, No, Alternate, or N/A]

6.8. Are Personnel Security practices routinely enforced, audited, and updated?

[Yes, No, Alternate, or N/A]

6.9. Are personnel required to complete formal SCRM training annually?

[Yes, No, Alternate, or N/A]

6.10. Are all personnel trained in security best practices? This includes, but is not limited to, insider threats, access control, and data protection.

[Yes, No, Alternate, or N/A]

6.11. Is there additional security training provided to users with elevated privileges?

[Yes, No, Alternate, or N/A]

6.12. Are you aware of security training practices performed by your sub-suppliers to their personnel?

[Yes, No, Alternate, or N/A]

6.12.1. If 'Yes', does it align with your security practices?

6.13. Do you have a Code of Conduct for your employees, suppliers and subcontractors?

[Yes, No, Alternate, or N/A]

6.13.1. Is the Code of Conduct always available and visible to your employees, suppliers, and subcontractors?

6.13.2. How [regularly or often] is this Code of Conduct updated? Please describe the frequency.

6.13.3. Do you have personnel designated to address questions or violations to the Code of Conduct?

6.13.4. Are these employees, suppliers, and subcontractors trained on the Code of Conduct, including privacy and confidentiality requirements, as required by your industry?

7. SUPPLY CHAIN INTEGRITY

7.1. Do your processes for product integrity conform to any of the following standards (e.g., ISO 27036, SAE AS6171, etc.)?

[Yes, No, Alternate, or N/A]

7.2. Do you control the integrity of your hardware/software (HW/SW) development practices by using Secure Development Lifecycle practices?

[Yes, No, Alternate, or N/A]

7.2.1. How do you manage the conformance of your third parties to your procedures?

7.3. Do you have documented performance and validation procedures for your HW/SW products or services?

[Yes, No, Alternate, or N/A]

7.3.1. What is your process to ensure conformance to those procedures?

7.3.1.1. How do you manage HW/SW products or service that are not in compliance with those procedures?

7.3.1.2. How are subcontractors held accountable to performance specifications?

7.3.2. What, if any, automated controls are in place for your validation processes?

7.3.2.1. How do you audit your validation processes?

7.4. Do you have processes in place to independently detect anomalous behavior and defects in HW/SW products or services?

[Yes, No, Alternate, or N/A]

7.4.1. What means do you provide to allow customers to report anomalies?

7.4.1.1. How do you monitor and track anomalous product or service behavior?

7.5. Do you monitor third-party HW/SW products or services for defects?

[Yes, No, Alternate, or N/A]

7.5.1. What are your processes for managing third-party products and component defects throughout their lifecycle?

7.6. Does the functional integrity of your product or services rely on cloud services (commercial or hybrid)?

[Yes, No, Alternate, or N/A]

7.6.1. What policies and procedures are in place to protect the integrity of the data provided through cloud services?

7.6.1.1. How do you manage the shared responsibility for cloud service integrity requirements with your suppliers?

7.7. Do you have required training on quality and product integrity processes for employees, suppliers, and subcontractors?

[Yes, No, Alternate, or N/A]

7.7.1. What mechanisms are in place for direct employees and contracted workers to ensure applicable training has been completed?

7.7.1.1. Do you pass down training requirements to your sub-suppliers, as applicable?

7.8. Do you have processes to evaluate prospective third-party suppliers' product integrity during initial selection?

[Yes, No, Alternate, or N/A]

7.8.1. What processes or procedures, if any, are in place to ensure that prospective suppliers have met your product integrity requirements?

7.8.1.1. How do your policies or procedures ensure appropriate management/leadership input on supplier selection decisions?

7.9. Do you have regularly scheduled audits to ensure compliance with HW/SW products or services integrity requirements?

[Yes, No, Alternate, or N/A]

7.9.1. What provisions for auditing are included within supplier contracts?

7.9.2. How do you pass down HW/SW products or services integrity requirements to third-party suppliers?

7.10. Do you have a process for improving integrity of HW/SW products or services?

[Yes, No, Alternate, or N/A]

7.10.1. What programs are in place to ensure continuous performance monitoring and improvement of key suppliers?

7.11. Do you have processes in place for addressing reuse and/or recycle of HW products?

[Yes, No, Alternate, or N/A]

7.11.1. What is your process?

8. SUPPLY CHAIN RESILIENCE

General

8.1. Does your organization have a formal process for ensuring supply chain resilience as part of your product offering SCRM practices?

[Yes, No, Alternate, or N/A]

8.1.1. What standards or industry frameworks do you use to help inform those practices?

8.2. Do you consider non-technical supply chain resilience threats such as weather, geo-political instability, epidemic outbreak, volcanic, earthquakes, etc.?

Supply Chain Disruption Risk Management (Business Continuity)

8.3. Do you maintain a formal business continuity plan necessary to maintain operations through disruptions and significant loss of staff?

[Yes, No, Alternate, or N/A]

8.3.1. If illness causes high absenteeism, are personnel cross-trained and able to perform multiple duties?

8.4. Do you maintain a formally trained and dedicated crisis management team, including on-call staff, assigned to address catastrophic or systemic risks to your supply chain or manufacturing processes?

[Yes, No, Alternate, or N/A]

8.4.1. Do you require and audit key suppliers for their ability to be prepared for unexpected supply chain disruptions?

8.5. Can personnel work remotely?

[Yes, No, Alternate, or N/A]

8.5.1. Do your service deliverables outline which services can be done remotely and which cannot?

8.5.1.1. Is that documented in Service-level agreement (SLA) or Terms and Conditions?

8.5.1.2. What infrastructure support is needed to support a shift to an at-home workforce?

Diversity of Supply Base

8.6. Does your company consider supplier diversity to avoid single sources and to reduce the occurrence of suppliers being susceptible to the same threats to resilience?

[Yes, No, Alternate, or N/A]

8.7. Does your company consider alternate offering delivery channels to mitigate extended supplier outages to include cloud, network, telecommunication, transportation, and packaging?

[Yes, No, Alternate, or N/A]

SIGNATURES:

Please include the names and titles of all persons completing this template.

Name: Date:

Title:

Signature: X____

Name: Date:

Title:

Signature: X____

Name: Date:

Title:

Signature: X____

Name: Date:

Title:

Signature: X____

Name: Date:

Title:

Signature: X____

APPENDIX A: REFERENCE MATERIALS

Qualifying Questions

Question 1.1

- NIST SP 800-53 (SA-12; SA-12 (1); SA-12 (2); SA (12(14); SA-11
- NIST IR 7622

Question 1.2

- NIST SP 800-161, ANSI/ASIS SCRM 1.2014, ISO 28000:2007, ISO 31000

SUPPLY CHAIN MANAGEMENT & SUPPLIER GOVERNANCE

Questions 2.2, 2.3

- ISO 9001:2015; NIST SP 800-161

Question 2.4

- FY19 NDAA Section 889 Prohibitions, U.S. Executive Order on Securing the Information and Communications Technology and Services Supply Chain 5/15/2019

Question 2.5

- NIST SP 800-161: PV-2; SA-12(13); NIST SP 800-53 (PV-2; SA-12(13))

Questions 2.6, 2.7

- NIST SP 800-53 (rev.4) (SA-12(1) Acquisition Strategies. Questions 1.13 - 1.19.1
- NIST SP 800-161 (SA-3): NIST SP 800-161, Chapter 2, page 21

Questions 2.8, 2.9

- NIST SP 800-53; NIST IR 7622; SIG LITE 2020; ISO 8.4; NIST SP 800-161 (IR-

SECURE DESIGN & ENGINEERING

Question 3.1

- N/A

Questions 3.2, 3.3

- BSIMM10: CP1.1, CP1.3, SR1.1, CP3.2, SM1.1, SM1.2, SM1.3, CP2.5, T1.1, T1.5, T1.7, T2.6, T2.8, T3.2, T3.4
- BSA: SC.1-1, SC.2, PD.1-1, PD.1-2, PD.1-3, PD.2-1, PD.2-2
- ISO 27034: 7.3.2
- MSSDL: Practice 1 & 2
- NISTCSF: ID.GV-3
- OWASPTEST: Phase 2.1
- PCISSLRAP: 1.1, 1.2, 1.3, 2.1

- SAMM15: PC1-A, PC1-B, PC2-A, SR1-A, SR1-B, SR2-B
- SCFPSSD: Planning the Implementation and Deployment of Secure Development Practices; Establish Coding Standards and Conventions
- SCAGILE: Operational Security Tasks 14, 15; Tasks Requiring the Help of Security Experts 1
- NIST SP 800- 53: SA-3, SA-8, SA-15
- NIST SP 800-160: 3.1.2, 3.2.4, 3.3.1, 3.4.2, 3.4.3
- NIST SP 800-181: T0414; K0003, K0039, K0044, K0157, K0168, K0177, K0211, K0260, K0261, K0262, K0524; S0010, S0357, S0368; A0033, A0123, A0151, T0001, T0004
- NISTCSF: ID.AM-6, ID.GV-2
- NISTCSF: PR.AT-*
- SP800160: 3.2.1, 3.2.4, 3.3.1
- SP800181: K0233
- SP800181: OV-TEA-001, OV-TEA-002; T0030, T0073, T0320; K0204, K0208, K0220, K0226, K0243, K0245, K0252; S0100, S0101; A0004, A0057
- SCSIC: Vendor Software Development Integrity Controls
- SAMM15: EG1-A, EG2-A, SM1.A

Question 3.4

- BSA: TV.2-1, TV.5-1, PD1-6
- BSIMM10: SM1.4, SM2.2
- ISO 27034: 7.3.5
- MSSDL: Practice 3
- OWASPTEST: Phase 1.3
- SAMM15: DR3-B, IR3-B, PC3-A, ST3-B
- NIST SP800-53: SA-15
- NIST SP800-160: 3.2.1, 3.2.5, 3.3.1, 3.3.7
- NIST SP800-181: K0153, K0165, T0349; K0153

Question 3.5

- BSA: TC.1, TC.1-1, TC.1-2, TC.1-6, PD.1.6
- MSSDL: Practice 8
- NIST SP800-53: SA-15
- NIST SP800-181: K0013, K00139, K0178
- SCAGILE: Tasks Requiring the Help of Security Experts 9
- SCAGILE: Tasks Requiring the Help of Security Experts 9
- PCISSLRAP: 2.5
- SCAGILE: Tasks Requiring the Help of Security Experts 9

Question 3.6

- BSA: IA.1, IA.2-2, SM.4-1
- IDASOAR: Fact Sheet 25
- NISTCSF: PR.AC-4
- OWASPASVS: 1.10, 10.3.2, 14.2
- PCISSLRAP: 6.1
- SCSIC: Vendor Software Delivery Integrity Controls, Vendor Software Development Integrity Controls

Question 3.7

- BSA: SM.4.2, SM.4.3, SM.5.1, SM.6.1
- BSIMM10: SE2.4
- NISTCSF: PR.DS-6
- PCISSLRAP: 6.2
- SAMM15: OE3-B
- SCSIC: Vendor Software Delivery Integrity Controls
- SP800181: K0178

Question 3.8

- IEC:IECEE, IECQ
- ISO 28000
- ISO 12931
- ISO 16678

Question 3.9

- BSA: PD.1-6,
- PD.1-5, TV.2, TV.3
- BSIMM10: CR1.2, CR1.4, CR1.6, CR2.6, CR2.7
- IDASOAR: Fact Sheets 3, 4, 5, 14, 15, 25, 48
- ISO 27034: 7.3.6
- MSSDL: Practices 9, 10
- NIST CSF: PR.IP-4
- NIST SP 800-53: SA-11, SA-15
- NIST SP 800-181: SP-DEV-002; K0013, K0039, K0070, K0153, K0165; S0174, SP-DEV-001, SP-DEV-002; T0013, T0111, T0176, T0267, T0516; K0009, K0039, K0070, K0140, K0624; S0019, S0060, S0078, S0137, S0149, S0167, S0174, S0242, S0266; A0007, A0015, A0036, A0044, A0047
- OWASPASVS: 1.1.7, 10
- OWASPTEST: Phase 3.2, Phase 4.1
- PCISSLRAP: 4.1, 5.2, 6.2

- SAMM15: IR1-B, IR2-A, IR2-B
- SCAGILE: Operational Security Tasks 4, 7
- SCFPSSD: Use Code Analysis Tools to Find Security Issues Early, Use Static Analysis Security Testing Tools, Perform Manual Verification of Security Features/Mitigations
- SCSIC: Peer Reviews and Security Testing & Vendor Software Delivery Integrity Controls

Question 3.10

- BSA: SC.1-3, SC.1-4, TV.3, TV.3-1, TV.5, SC.2, SC.4, SC.3, SC.3-2, EE.1, EE.1.2, EE.2, LO.1
- BSIMM10: AM1.3, AM1.5, AM2.1, AM2.2, AM2.5, AM2.6, AM2.7, AA1.2, AA2.1
- IDASOAR: Fact Sheet 1
- ISO 27034: 7.3.3, 7.3.5
- MSSDL: Practice 4 & 9
- NISTCSF: ID.RA-*
- NIST SP 800-53: SA-8, SA-15, SA-17
- NIST SP 800-160: 3.3.4, 3.4.5
- NIST SP 800-181: T0038, T0062, T0236, T0328; K0005, K0009, K0038, K0039, K0070, K0080, K0119, K0147, K0149, K0151, K0152, K0160, K0161, K0162, K0165, K0172, K0297, K0310, K0344, K0362, K0487, K0624; S0006, S0009, S0022, S0036,S0078, S0141, S0171, S0229, S0248; A0092, A0093, A107
- NIST SP-DEV-001; T0013, T0077, T0176; K0009, K0016, K0039, K0070, K0140, K0624; S0019, S0060, S0149, S0172, S0266; A0036, A0047
- OWASPASVS: 1.1.2, 1.2, 1.4, 1.5, 1.6, 1.7, 1.8, 1.9, 1.11, 2 through 13
- OWASPTEST: Phase 2.4
- PCISSLRAP: 3.2
- SAMM15: DR1-A, DR1-B, TA1-A, TA1-B, TA3-B
- SCAGILE: Tasks Requiring the Help of Security Experts 3
- SCFPSSD: Threat Modeling, Establish Log Requirements and Audit Practices, Handle Data Safely, Handle Errors, Use Safe Functions Only
- SCTTM: Entire guide

Question 3.11

- BSA: SM.1, SM.2, SM.2-1, SM.2.4, SC.3-1, TV.2
- BSIMM10: CP2.4, SR2.5, SR3.2
- IDASOAR: Fact Sheets 19, 21
- NIST SP 800-53: SA-4, SA-12
- NIST SP 800-160: 3.1.1, 3.1.2, 3.3.8
- NIST SP 800-181: T0203, T0415; K0039; S0374; A0056, A0161; SP-DEV-002; K0153, K0266
- MSSDL: Practice 7
- OWASPASVS: 10, 14.2

- PCISSLRAP: 4.1
- SAMM15: SR3-A
- SCFPSSD: Manage Security Risk Inherent in the Use of Third-Party Components
- SCSIC: Vendor Sourcing Integrity Controls
- SCAGILE: Tasks Requiring the Help of Security Experts 8
- SCTPC: 3.2.2

Question 3.12

- BSA: SM.2, SM.2.1, SI.2, EN.1-1, LO.1
- BSIMM10: SFD1.1, SFD2.1
- IDASOAR: Fact Sheet 19
- MSSDL: Practice 5 & 6
- NIST SP 800-53: SA-12
- NIST SP 800-181: K0039, SP-DEV-001
- OWASPASVS: 10, 1.1.6
- SAMM15: SA1-A
- SCTPC: 3.2.1
- SCFPSSD: Establish Log Requirements and Audit Practices

Question 3.13

- BSA: TC.1-1, TC.1-3, TC.1-4, TC.1-5
- MSSDL: Practice 8
- NIST SP 800-181: K0039, K0070
- OWASPASVS: 1.14.3, 1.14.4, 14.1
- SCAGILE: Operational Security Task 3 & 8
- SCFPSSD: Use Current Compiler and Toolchain Versions and Secure Compiler Options
- SCSIC: Vendor Software Development Integrity Controls
- SCFPSSD: Use Current Compiler and Toolchain Versions and Secure Compiler Options

Question 3.14

- BSA: PD.1-5, TV.3, TV.5, TV.5-2, VM.1-3, VM.3
- BSIMM10: PT1.1, PT1.2, PT1.3, ST1.1, ST1.3, ST2.1, ST2.4, ST2.5, ST2.6, ST3.3, ST3.4
- IDASOAR: Fact Sheets 7, 8, 10, 11, 38, 39, 43, 44, 48, 55, 56, 57
- ISO 27034: 7.3.6
- NIST SP 800-53: SA-11, SA-15
- NIST SP 800-181: SP-DEV-001, SP-DEV-002; T0456; K0013, K0039, K0070, K0153, K0165, K0342, K0367, K0536, K0624; S0001, S0015, S0026, S0061, S0083, S0112, S0135, T0028, T0169,

T0176, T0253, T0266, T0516; K0009, K0039, K0272, K0339, K0342, K0362, K0536; S0046, S0051, S0078, S0081, S0083, S0135, S0137, S0167, S0242; A0015

- MSSDL: Practice 11
- PCISSLRAP: 4.1
- SAMM15: ST1-B, ST2-A, ST2-B
- SCAGILE: Operational Security Tasks 10, 11; Tasks Requiring the Help of Security Experts 4, 6, 7
- SCFPSSD: Perform Dynamic Analysis Security Testing, Fuzz Parsers, Network Vulnerability Scanning, Perform Automated Functional Testing of Security Features/Mitigations, Perform Penetration Testing
- SCSIC: Peer Reviews and Security Testing

Question 3.15

- BSA: CF.1, TC.1
- IDASOAR: Fact Sheet 23
- ISO 27034: 7.3.5
- OWASPTEST: Phase 4.2
- SCAGILE: Tasks Requiring the Help of Security Experts 12
- SCSIC: Vendor Software Delivery Integrity Controls, Vendor Software Development Integrity Controls
- NIST SP 800-181: SP-DEV-002; K0009, K0039, K0073, K0153, K0165, K0275, K0531; S0167, SP-DEV-001
- PCISSLRAP: 8.1, 8.2
- SCFPSSD: Verify Secure Configurations and Use of Platform Mitigation

Question 3.16

- BSA: VM.2, VM.2-1, VM.2-2, VM.1-1, VM.2-3, VM.2-4
- SCAGILE: Tasks Requiring the Help of Security Experts 10
- NIST SP 800-53: SA-10
- NIST SP 800-160: 3.3.8
- NIST SP 800-181: K0009, K0039, K0070, K0161, K0165; S0078
- PCISSLRAP: 4.1, 4.2
- SCAGILE: Operational Security Task 2
- SCFPSSD: Fix the Vulnerability, Identify Mitigating Factors or Workarounds
- SP800181: T0163, T0229, T0264; K0009, K0070

Question 3.17

- BSA: VM.2-1, PD.1-3
- BSIMM10: CMVM3.2
- MSSDLPG52: Phase Two: Design
- MSSDL: Practice 2

- NIST SP800181: T0047, K0009, K0039, K0070, K0343
- NIST SP800160: 3.3.8
- NIST SP800181: T0111, K0009, K0039, K0070, K0343, SP-DEV-001, SP-DEV- 002; K0009, K0039, K0070
- PCISSLRAP: 2.6, 4.2
- SAMM15: IM3-A
- SP800181: K0009, K0039, K0070

INFORMATION SECURITY

Question 4.1

- ISO 27001
- SOC 2 Type II
- CMMC Level 3-5, Cybersecurity Maturity Assessment

Question 4.2

- ISO IEC 27001, ISO 20243, ISO 27036
- NIST CSF1.1
- NIST 800-37, Rev. 2
- NIST SP 800-161
- SAE AS649, etc.

Question 4.3

- European Union General Data Protection Regulation (GDPR) regulation April 2016

Question 4.4

- NIST 800-53, NIST 800-171 DFARS, ISA/IEC 62443 or ISO 28001/2
- ISO 27003:2013 sec. 7.5.3, 8.2.2, 8.2.3, 8.3.1,14.1.2
- NIST SP 800-192: High-level requirements that specify how access is managed and who may access information under what circumstances.
- CNSSI 4009-2015 under multifactor authentication NIST SP 800-53 Rev. 4: Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). See authenticator.
- ISO 27003:2013 sect 9.2.1, 12.2.1, 13.1.1, Shared Assessments Standardized Control Assessment (SCA) sect. T.1
- Shared Assessments Standardized Control Assessment (SCA) sect. M.1
- NIST SP 800-12 Rev. 1 under Encryption ISO 7498-2: The cryptographic transformation of data to produce ciphertext.
- ISO 27003:2013 sect 10.1.2

Question 4.5

- CCMM:ID.AM
- ISA 99: 4.2.3.4 & SR 7.8, ISO 27001: A.8.1.1, A.8.1.2
- NIST CSF1.1
- NIST 800-53: CM8, CCS:2, BAI09.01, BAI09.02, BAI09.05

Question 4.6

- NIST 800-53 r5: RA-57

Question 4.7

- CCMM:ID.AM
- ISA 99: 4.2.3.4 & SR 7.8
- ISO 27001: A.8.1.1, A.8.1.2
- NIST CSF1.1
- NIST 800-53: CM8, CCS:2, BAI09.01, BAI09.02, BAI09.05

Question 4.8

- CCMM: ID.AM
- ISA 99: 4.2.3.4 & SR 7.8, ISO27001: A.8.1.1, A.8.1.2
- NIST CSF1.1, NIST 800-53: CM8, CCS:2, BAI09.01, BAI09.02, BAI09.05

Question 4.9

- NIST SP 800-60 r1

Question 4.10

- NIST 800-53 r5: SI 7(12)

Question 4.11

- NIST 800-53 r5:SI-5, PM – 16

Question 4.12

- CCMM: EDM1
- NIST 800-53:PL2, SA1
- CCMM: CPM3
- NIST 800-161 PE-16 Delivery and Removal,
- PE-17 Alternate Work Site,
- PE-18 Location of Information System Components)
- ISO 27001 A.11.1.6 - Delivery and loading areas
- A.11.2.3 - Cabling security
- A.11.2.8 - Unattended user equipment

Question 4.13

- NIST SP 800-53 r4: SI-12

Question 4.14

- NIST SP 800-128 under Vulnerability
- CNSSI 4009
- ISO 27003:2013 sect. 12.6.1
- Shared Assessments Standardized Control Assessment (SCA) sect. T.4

Question 4.15

- CNSSI 4009-2015
- ISO 27003:2013 sect 9.2.1, 12.2.1, 13.1.1, Shared Assessments Standardized Control Assessment (SCA) sect. T.1
- NIST SP 800-192
- NIST SP 800-53 Rev. 4: Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). See authenticator.
- Shared Assessments Standardized Control Assessment (SCA) sect. M.1

Question 4.16

- ISO 27003:2013 sect. 7.2.2

Question 4.17

- DFARS 252.246-7007

Question 4.18

- NIST SP 800-12 Rev. 1 under Encryption
- ISO 7498-2
- ISO 27003:2013 sect 10.1.2

Question 4.19

- NIST SP 800-152
- ISO 27003:2013 sect 9.1.2, 13.1.1
- ISO 27003:2013 sect13.1.3, Shared Assessments Standardized Control Assessment (SCA) sect. N.3
- NIST 800-53 or related controls
- NIST SP 800-152: A process intended to eliminate a means of attack by patching vulnerabilities and turning off nonessential services.
- https://csrc.nist.gov/glossary/term/operational_technology

Question 4.20

- Shared Assessments Standardized Control Assessment (SCA) sect. V.2

Question 4.21

- ISO 27003:2013 sect 16.1.1

Question 4.22

- NIST SP 800-37 rev 2
- NIST SP 800-95: A method of testing where testers target individual binary components or the application, in whole, to determine whether intra or inter component vulnerabilities can be exploited to compromise the application, its data, or its environment resources.

Question 4.23

- Shared Assessments Standardized Control Assessment (SCA) sect. U.1

Question 4.24

- NIST CSF1.1

Question 4.25

- CNSSI 4009-2015 under incident handling
- NIST SP 800-61 Rev. 2.
- Shared Assessments Standardized Control Assessment (SCA) sect. K.4

Question 4.26

- Shared Assessments Standardized Control Assessment (SCA) sect. K.5

Question 4.27

- N/A

PHYSICAL SECURITY

Question 5.1

- DoD 5220.22-M, February 28, 2006 (National Industrial Security Program Operating Manual) Incorporating Change 2, May 18, 2016 (all applicable chapters, section, paragraphs).

Question 5.2

- NIST 800-53, rev. 4, PE-1, PE-2, PE-3.
- NIST Special Publication 800-53 Revision 3 PE-1, 2, 3
- American Petroleum Institute Pipeline SCADA Security Standard API 1164 2nd Edition 4, Annex A
- North American Electric Reliability Corporation (NERC) CIPS CIP 006-3c, A, B, R1
- NRC Cyber Security Programs for Nuclear Facilities Regulatory Guide 5.71 App. B.1.1, App. C.5.1
- ISO 27001 (specific clause desired here)
- NASA - CS-10 - Physical security measures - documented. Audited
- NASA - CS-11 - Physical access controls - documented and audited
- NASA- CS-15 - Background checks

Question 5.3

- ONSAT-PSP-14.3
- NIST 800-161 AT-3 - Security Training
- NASA -CS-4, incident response

Question 5.4

- Department of Homeland Security's (DHS) Cyber Security Evaluation Program (CSEP) – CRR implementation guide: sect. 5 Incident Mgmt

Question 5.5 - Source of Question – ONSAT-PSP-14.5

- ONSAT-SDV-18.1
- NIST 800-161 (AC)

Questions 5.6, 5.7

- NIST 800-161 AC-3, PE-20
- NSIT 800-161 PE-3 Physical Access Control including tamper protection
- PE-20 Asset Monitoring and Tracking
- CM-8 Information System Component Inventory
- SA-18 Tamper Resistance and Detection
- SA-17 Developer Security Architecture
- SC-36 Distributed Processing and Storage)
- ISO 27001 - A.11.1.1 - Physical security perimeter
- A.11.1.1.2 - Physical Entry controls
- A.11.1.3 - Securing Offices, rooms and facilities·
- A.11.2.5 - Removal of assets
- NASA - CS-9 - Tamper resistant
- NASA - CS-10 - Physical Security measures in place
- NASA CS-11 - Access controls in place

Question 5.8

- NIST SP 800-53 (PV-2; SA-12(13))

Question 5.9

- NIST SP 800-53 (rev.4) (SA-12(1) Acquisition Strategies. Questions 1.13 - 1.19.1

Question 5.10

- IEC:IECEE, IECQ
- ISO 28000
- ISO 12931
- ISO 16678

PERSONNEL SECURITY

Questions 6.1 – 6.13

- BSA: PD.2-1, PD.2-2
- BSIMM10: CP3.2, SM1.1
- NISTCSF: ID.AM-6, ID.GV-2
- PCISSLRAP: 1.2
- SCSIC: Vendor Software Development Integrity Controls
- SP80053: SA-3
- SP800160: 3.2.1, 3.2.4, 3.3.1
- SP800181: K0233
- BSA: PD.2-2
- BSIMM10: CP2.5, SM1.3, T1.1, T1.5, T1.7, T2.6, T2.8, T3.2, T3.4
- MSSDL: Practice 1
- NISTCSF: PR.AT-*
- PCISSLRAP: 1.3
- SAMM15: EG1-A, EG2-A
- SCAGILE: Operational Security Tasks 14, 15; Tasks Requiring the Help of Security Experts 1
- SCFPSSD: Planning the Implementation and Deployment of Secure Development Practices
- SCSIC: Vendor Software Development Integrity Controls
- SP80053: SA-8
- SP800160: 3.2.4
- SP800181: OV-TEA-001, OV-TEA-002; T0030, T0073, T0320; K0204, K0208, K0220, K0226, K0243, K0245, K0252; S0100, S0101; A0004, A0057
- BSIMM10: SM1.2, SM1.3
- PCISSLRAP: 1.1
- SAMM15: SM1.A
- SP 800-181: T0001, T0004
- CDSE document on planning for Insider Threat program - https://www.cdse.edu/documents/cdse/sample-insider-threat-program-plan-for- industry.pdf
- NIST Cybersecurity Framework (2018) - https://www.nist.gov/cyberframework

SUPPLY CHAIN INTEGRITY

Question 7.1

- ISO 27036
- SAE AS6171

Question 7.2

- Microsoft's Trustworthy Computing Security Development Lifecycle, TSP for Secure Software Development

Question 7.3

- ONSAT - SDI 2.4

Question 7.4

- ONSAT - SDI 2.3

Question 7.5

- ISO 27036

Question 7.6

- NIST.SP.500-291r2 sect 6.5

Question 7.7

- ISO 27036, ONSAT – PSP 14.1

Question 7.8

- ISO 27036

Question 7.9

- ISO 27036
- ONSAT – AIA 4.1

Question 7.10

- ONSAT – AIA 4.1

Question 7.11

- R2:2013 - Sustainable Electronics Recycling International, sect 15

SUPPLY CHAIN RESILIENCE

Questions 8.1, 8.2

- Consistent with EO 13873 CISA Guidance (4/2020) and Supply Chain resilience
- Identify the people: 2. Manage the security and compliance: 3. Assess the components 4. Know the supply chain and suppliers. 5. Verify assurance of third parties. 6. Evaluate your SCRM program.

Questions 8.3, 8.4, 8.5

- NIST 800-161 (CP-8(4))
- NIST 800-161 (CP-8(3))

Questions 8.6, 8.7

- NIST 800-161 (PL-8(2))

- NIST 800-161 (PL-8(2)); Threat scenario 1 (Appendix B)

APPENDIX B: SUPPLEMENTAL INFORMATION (REASONING AND RATIONALE)

1. Qualifying Question

- **Question 1.1** – These qualifying questions provide flexibility to respond to the survey by providing evidence of previous template submission or by providing evidence of qualifying SCRM industry or government certifications held by the responding organization.

2. Supply Chain Management and Supplier Governance

- **Question 2.1** – This question is probing to ensure policies are regularly updated and communicated to customers to ensure regular maintenance of established processes/procedures for SCRM.
- **Questions 2.2, 2.3** - These questions ask whether the supplier has policies and procedures in place to address supply chain risks. If the company is fully compliant with ISO 9001, then we may have more confidence in their implementation, auditing, training, and change management processes. If the company is not fully compliant with ISO 9001, then we will have to dig deeper to understand whether they have effective implementation, audit plans, training, change management processes, etc. Supply chain risks can be introduced at any point in the SDLC. We need to ensure that the supplier is thinking about its supply chain throughout the lifecycle.
- **Question 2.4** - Ability to identify, track and validate that no components banned by the country of receipt reduces risk of receipt of vulnerable products/components, counterfeits and products or components that have been intentionally tampered with by bad actors.
- **Question 2.5** - These questions ask about the provenance of products and services to help manage supply chain risks, such as "unauthorized tampering and modification through the ICT supply chain, especially during repairs/refurbishing, updating," risks associated with lack of diversity, etc. Additionally, when invoking a SAAS capability, we recommend that the SBOM of the service is available to the user for local archive/logging for later analysis, in the event, that vulnerabilities are later identified.
- **Questions 2.6, 2.7** - These questions seek to understand aspects of BOM such as what attributes are in the BOM, what is being tracked, etc. We recognize that companies may need different categories in a BOM. For example, some companies may need "critical components" that may include customized components, components mounted with multiple other components, etc.
- **Questions 2.8, 2.9** - Stakeholders want to know that the supplier not only has a comprehensive and robust SCRM program for itself (which helps us to mitigate our own risk and meet customer expectations), but that it also requires the same from its sub-suppliers. We also want to ensure that the supplier ensures that "externally provided processes, products and services" conform to the SCRM requirements expected from the supplier and ensure that the supplier can meet the expectations of its customers. Suppliers must establish incident handling, including preparation, detection analysis, containment and recovery. We want incidents to be addressed with appropriate mitigations. Finally, we want to ensure that we are notified of changes in subcontractors because those changes could impact our ability to appropriately identify our own supply chain risks and our ability to meet the customers' expectations.

3. Secure Design and Engineering

- **Question 3.1** - The ICT SCRM WG#4 System Design Writing Team identified questions that vendors might reasonably be asked to answer and/or elaborate upon with respect to their software and system design practices. The National Institute of Standards and Technology's

Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF) white paper is the source for nineteen questions spanning four categories. The questions in this document are lifted nearly verbatim from the SSDF and arranged such that a lightweight Yes/No/Alt/NA response to each question would suffice for a simple inquiry. However, each question is also paired with a deeper question, which would be appropriate for a deeper inquiry and elicit a more elaborate response than a simple Yes, No, Alternate, or Not Applicable answer. Finally, the SSDF mappings to other documents and frameworks were also included as references to help vendors and evaluators. One question that was not taken from the SSDF is the "Level 0" question which (dis)qualifies the vendor from answering any questions in this section.

- **Question 3.2** – N/A
- **Questions 3.3, 3.4** - Risk/Rationale: This includes requirements from internal sources (e.g., the organization's policies, business objectives, and risk management strategy) and external sources (e.g., applicable laws and regulations).
- **Question 3.5** - Risk/Rationale: Toolchains and tools may be used at different levels of the organization, such as organization-wide or project-specific.
- **Question 3.6** - Risk/Rationale: For code that is not intended to be publicly accessible, it helps prevent theft of the software and may make it more difficult or time-consuming for attackers to find vulnerabilities in the software.
- **Question 3.7** – N/A
- **Question 3.8** – N/A
- **Question 3.9** – N/A
- **Question 3.10** - Risk/Rationale: Addressing security requirements and risks during software design (secure by design) helps to make software development more efficient. These are particularly true for software that implements security functionality, such as cryptographic modules and protocols.
- **Question 3.11** – N/A
- **Question 3.12** – N/A
- **Question 3.13** – N/A
- **Question 3.14** - Risk/Rationale: Using automated methods lowers the effort and resources needed to detect vulnerabilities. Human-readable code includes source code and any other form of code an organization deems as humanly readable. Executable code includes binaries, directly executed bytecode, directly executed source code, and any other form of code an organization deems as executable.
- **Question 3.15** – N/A
- **Question 3.16** – N/A
- **Question 3.17** – N/A

4. Information Security

- **Question 4.1** – Risk/Rationale: there is no independent evaluation of holistic cybersecurity processes which meeting industry standards.
- **Question 4.2** – Risk/Rationale: Ad hoc or untested or incomplete/insufficient controls

- **Question 4.3** – Risk/Rationale: Lack of privacy controls can be assumptions of other types of missing information security controls. Companies at risk for EU GDPR violations, could suffer financial harm.
- **Question 4.4** – Risk/Rationale: Contaminated backups. Contamination of backup assets can slow recovery and prevent full restoration.
- **Question 4.5** – Risk/Rationale: Inadequate scope of procedures for managing enterprise network-connected assets.
- **Question 4.6** – Risk/Rationale: Non-IT professionals may bring in malware/viruses unintentionally from external downloads.
- **Question 4.7** – Risk/Rationale: Unable to identify rogue or at-risk equipment or inability to distribute patches in a timely manner.
- **Question 4.8** – Risk/Rationale: Unmanaged assets could be tampered with at any point in their lifecycle
- **Question 4.9** – Risk/Rationale: Lack of legal/regulatory compliance and potential security risk of using a product produced by a company on a banned list.
- **Question 4.10** – Risk/Rationale: Accidental or intentional introduction of vulnerabilities that could lead to failure or exploitation of mission critical functions
- **Question 4.11** – Risk/Rationale: No repeatable means of proactively identifying cybersecurity breaches. Lack of early detection of attacks, Lack of vetted detection techniques, etc.
- **Question 4.12** – Risk/Rationale Ensure physical security is coordinated with Information Security. May not apply to organizations that manage all valuable/critical cyber assets in a virtual environment. Reducing the risk of a cyber-attack on physical security systems and controls.
- **Question 4.13** – Risk: Breach of confidentiality ISO 27003:2013 sect 7.5.3
- **Question 4.14** – Risk/Rationale: Remote exploit or lateral exploit
- **Question 4.15** – Risk/Rationale: Unauthorized access. Nonstandard, non- comprehensive access control policies or procedures.
- **Question 4.16** – Risk/Rationale: Social Engineering, Carelessness, Adherence to Policy
  - **Question 4.16.1** – Risk/Rationale: If not refreshed, likely policies are not being consistently followed.
  - **Question 4.16.2** – Risk/Rationale: Improper/untrained access. Third-party workers accessing the same data as employees without proper training.
- **Question 4.17** – Risk/Rationale: Data Liability, Confidentiality
- **Question 4.18** – Risk/Rationale: Confidentiality of sensitive data
  - **Question 4.18.1** – Risk/Rationale –Some encryption keys can become a vulnerability source if not comprehensively managed.
  - **Question 4.18.2** – Risk/Rationale – Incomplete mitigation of risk if only data at rest or data in transit is protected.
- **Question 4.19** – Risk/Rationale: Remote exploit or lateral exploit.
- **Question 4.20** – Risk/Rationale: Presumed transfer of risk to cloud.
- **Question 4.21** - Risk/Rationale: Delay in, or inability to, recover.
- **Question 4.22** – Risk/Rationale: Undetected vulnerability.

- **Question 4.23** – Risk/Rationale: Patch management and detection of unauthorized software/releases (delta to inventory).
- **Question 4.25** – Risk/Rationale: Operational continuity during/after an attack.
- **Question 4.26** – Risk/Rationale: lack of ability to fully recover and validate system integrity. Loss of critical inputs from single or limited source suppliers (JIT Sensitivity).
- **Question 4.27** – Risk/Rationale: Customer could become liable for recovery costs.

5. Physical Security

Physical security is a mature activity however it has become more reliant on electronic and network connected systems. It is increasingly challenging to prevent overlapping of physical, cyber, and personnel security concerns as businesses become more reliant on Identity and Access Management (IDAM) systems to control facility access and report intrusion attempts. These systems which can update personnel status immediately and whose data flows across the organization's networks have demonstrated the need for these security "silos" to be more closely integrated.

Traditional physical security roles still exist, guards still have a role, but that role may require more understanding of how cyber-attacks work and behaviors associated with a trusted insider seeking to commit a malicious act. The ability of a guard to question, observe, and accurately report information may be highly relevant to a personnel or cyber security incident. Below is information about the reasoning behind the questions in the template.

- **Question 5.1** – Risk/Rationale: Green light questions that subsume most of the following questions (4.2-4.9).
- **Question 5.2** – Risk/Rationale: To ensure the company has policies and procedures that address the risk of how physical security responsibility includes and places a very high priority on preventing unauthorized access to cyber assets.
    - **Question 5.2.1** – Risk/Rationale: Not all policies and procedures are aligned with standards but if they are, this information is useful to understand the degree to which the policies may be effective.
- **Question 5.3** – Risk/Rationale: Ensure trustworthiness of individuals. Staff with non-cyber responsibilities may not be aware of the possible impact of seemingly inconsequential actions. Cybersecurity staff may not understand the full breadth of threats to the enterprise and how such threats may manifest as cyber impacts.
- **Question 5.4** – Risk/Rationale: Protection from a potential loss of revenue, reputation, and customer trust. Data protection is important both personally and professionally.
- **Question 5.5** – Risk/Rationale: A policy should direct responsibility and accountability. Those responsible and accountable should ensure that effective procedures to follow are established and promulgated to all staff. Cybersecurity staff may need to correlate physical security awareness with cybersecurity-related activity. Ensure the policy has been exercised to demonstrate its effectiveness in recovering from a potential incident.
- **Questions 5.6, 5.7** – Risk/Rationale: Ensure only authorized individuals have access to the facility, also ensure policies are documented. While a single mistake by an individual who harbors no malicious intent may warrant an informational sanction (i.e. warning) multiple breeches of security or other patterns may be important indicators of a significant risk. Having a formal policy and set of procedures reduces the likelihood that such a risk would go unnoticed?
- **Questions 5.8 – 5.10** These questions ask about the provenance of products and services to help manage supply chain risks, such as "unauthorized tampering and modification through the ICT

supply chain, especially during repairs/refurbishing, updating," risks associated with lack of diversity, etc. Additionally, when invoking a SAAS capability, we recommend that the SBOM of the service is available to the user for local archive/logging for later analysis, in the event, that vulnerabilities are later identified.

6. Personnel Security

- **Question 6.1** "General" questions intend to identify processes, policies, and documents on personnel as it relates to purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance for information security. (NIST 800-53, Page F145).
- **Questions 6.2 - 6.5** "Onboarding" questions intend to measure how during the initial point of entry for new employees, they are introduced to the organization's security principles and culture.
  - **Question 6.6** "Offboarding" questions intend to illustrate the organization's preparedness with the potential risk(s) for terminated/discharged employees.
- **Questions 6.7- 6.13** "Awareness and Training" questions intend to meet the NIST CSF (2018) requirements and definition – the organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements. (NIST CSF, 2018, Page 31)

7. Supply Chain Integrity

These questions check whether the supplier knows the companies in its own supply chain and has vetted those companies. This will help to mitigate supply chain risks such as diversity of our supply chain, geopolitical risks, etc. We also want to check whether the supplier vets the employees of their suppliers who might be provided as part of the service. This will help us to mitigate supply chain risks that stem from those employees (insider threats, etc.)

- **Question 7.1** – Risk/Rationale: Product visibility and traceability may not be comprehensive if not aligned to any frameworks or standards
- **Question 7.2** – Risk/Rationale: Lack of use of SDL could result in security vulnerabilities being missed somewhere within the lifecycle and inability to detect flaws early.
- **Question 7.3** – Risk/Rationale: Lack of documented validation processes creates an inability to detect product quality failures. Lack of proper disposition of non-conforming materials can result in release to customers.
- **Question 7.4** - Risk/Rationale: Lack of detection processes creates an inability to detect counterfeit product or product that has been tampered. Failure to notify customers could exacerbate impacts.
- **Question 7.5** – Risk/Rationale: Third-party HW/SW products may not have as stringent quality control and defect analysis and therefore could be at higher risk for non-conformance or being counterfeit.
- **Question 7.6** – Risk/Rationale: Cloud developed software poses additional potential integrity vulnerabilities due to possible data breach, account hijacking, poor credential management, and potential system vulnerabilities among other threats. Lack of proper controls on critical cloud infrastructures can result in unintended or unmanaged vulnerabilities for the end-product or service.

- **Question 7.7** - Risk/Rationale: Lack of regular and tracked training for all direct personal and relevant supplier personnel could lead to product integrity processes not being followed.
- **Question 7.8 –** Risk/Rationale: Lack of evaluation of a supplier's product integrity could introduce undesired integrity vulnerabilities. Management reviews of supplier selection choices provide additional controls.
- **Question 7.9 –** Risk/Rationale: Regular audits ensure that processes are being performed and running as desired and offer opportunities for improvements. Passing down audit requirements to suppliers ensures supplier integrity of your suppliers.
- **Question 7.10 –** Risk/Rationale: On-going re-evaluation of integrity processes enables incorporation of changing standards, response to changing product requirements and a culture of continuous improvement.
- **Question 7.11 –** Risk/Rationale: Lack of controlled disposal procedures could increase risks of counterfeiting and unintended uses.

8. Supply Chain Resilience

- **Questions 8.1 – 8.2** "Supply chain resilience" is defined as the ICT supply chain's ability to provide required ICT products and services under stress or failure (NIST 800-161, Page 3).The General questions are intended to measure the extent to which the company has a program in place to assess the architecture of its Critical ICT elements and assets.
- **Questions 8.3 – 8.5** "Business Continuity" questions are intended to address new concerns for organizations moving to remote or reduced work environments due to unplanned events. The questions are intended to ensure the presence of robust business continuity plans.

  Questions 8.6 – 8.7 The "supplier diversity" questions are intended to measure the processes companies use to limit the event of multiple suppliers being susceptible to the same threats (*e.g.,* geographic supplier diversity program.)