CYBER SUPPLY CHAIN RISK MANAGEMENT QUESTIONNAIRE

Table of Contents

Introduction

The questions in this form are based on the operational requirements of the NIST SP 800-161 standard, **Supply Chain Risk Management Practices for Federal Information Systems and Organizations [csrc.nist.gov]** and ISO/IEC 27036 standard, **Information Security for Supplier Relationships [iso.org]**

The following is an abstract of the NIST SP 800-161 publication:
"Federal agencies are concerned about the risks associated with information and communications technology (ICT) products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the ICT supply chain. These risks are associated with the federal agencies decreased visibility into, understanding of, and control over how the technology that they acquire is developed, integrated and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services. This publication provides guidance to federal agencies on identifying, assessing, and mitigating ICT supply chain risks at all levels of their organizations. This publication integrates ICT supply chain risk management (SCRM) into federal agency risk management activities by applying a multitiered, SCRM-specific approach, including guidance on supply chain risk assessment and mitigation activities."
The following is an abstract of the ISO/IEC 27036 publication: "ISO/IEC 27036 is a multi-part standard offering guidance on the evaluation and treatment of information risks involved in the **acquisition of goods and services from suppliers.** The implied context is business-to-business relationships, rather than retailing, and information-related products. The terms acquisition and acquirer are used rather than purchase and purchasing since the process and the risks are much the same whether or not the transactions are commercial (e.g. one part of an organization or group may acquire products from another part as an internal transfer without literally paying for them)."
Please review the above document when responding to the questions in this form. Thank you for the time and attention your organization has applied to completing this form.

Form Submission

First Name :

Last Name :

Job Title :

Email Address:

Form Questions

1-1. Does your Organization follow industry best practices for Supply Chain Risk Management (SCRM)?

○ Yes-Fully
○ Yes-Partially
○ No

1-2. Provide additional descriptive information on the best practices being followed

□

1-3. If the response to Question 1-1 is No, does your organization have a roadmap over the next 3-5 years to become fully or partially compliant with industry best practices for Supply Chain Risk Management (SCRM)?

○ Yes-Fully
○ Yes-Partially
○ No

1-4. Provide additional descriptive information regarding your organizations roadmap to become fully or partially compliant

□

2-1. Does your organization employ techniques and processes to safeguard component manufacturing designs against unauthorized or uncontrolled disclosure?

○ Yes-Fully
○ Yes-Partially
○ No

2-2. Provide additional descriptive information on the techniques and processes used to safeguard against unauthorized or uncontrolled disclosure

□

3-1. Does your organization employ techniques and practices for conducting vulnerability assessments on your products software, firmware and/or hardware components?

○ Yes-Fully
○ Yes-Partially
○ No

3-2. Provide additional descriptive information on various techniques and practices used

□

4-1. Does your organization qualify and periodically re-assess 3rd party key suppliers and/or business partners for compliance against the same Supply Chain Risk Management (SCRM) best practices you follow?

○ Yes-Fully
○ Yes-Partially
○ No

4-2. Provide additional descriptive information on requirements and frequency of assessments

□

4-3. If the response to Question 4-1 is No, does your organization have a roadmap over the next 1-2 years to qualify and implement a re-assessment approach for your 3rd party key suppliers and business partners for compliance against the same Supply Chain Risk Management (SCRM) best practices you follow?

○ Yes-Fully
○ Yes-Partially
○ No

4-4. Provide additional descriptive information regarding your organization’s roadmap for assessments

□

5-1. Do you employ Malware detection on software or firmware components of your products before final packaging and delivery?

○ Yes-Fully
○ Yes-Partially

○ No
○ N/A

5-2. Provide additional descriptive information on Malware detection on software or firmware components employed by your organization

□

6-1. Do your products include Tamper-Proof Modules (TPM) or employ similar means (e.g. Known Answer Test – KAT or Pairwise Consistency Test - PWCT) to detect tampering or the insertion of tainted, compromised or unauthorized components within a product architecture?

○ Yes-Fully
○ Yes-Partially
○ No

6-2. Provide additional descriptive information on method(s) used to detect tampering or the insertion of tainted, compromised or unauthorized components within a product architecture

□

6-3. If the answer to Question 6-1 is Yes or Yes-Partially, does your supplier provide trusted attestation around the validity of firmware and software components for its devices?

○ Yes-Fully
○ Yes-Partially
○ No

6-4. Provide additional descriptive information on method of trusted attestation around the validity of firmware and software components from suppliers

□

7-1. Does your organization use secure transmission and handling of hardware assets and artifacts for delivery of your products while in transit to their destination?

○ Yes-Fully
○ Yes-Partially
○ No

7-2. Provide additional descriptive information regarding method of secure transmission and handling of hardware assets and artifacts for delivery of your products while in transit

8-1. Does your organization use secure transmission and handling of software or firmware assets and artifacts for delivery of your products while in transit to their destination?

○ Yes-Fully
○ Yes-Partially
○ No

8-2. Provide additional descriptive information regarding method of secure transmission and handling of software or firmware assets and artifacts for delivery of your products while in transit

9-1. Does your organization perform supply chain risk or security awareness training periodically to your employee population?

○ Yes-Fully
○ Yes-Partially
○ No

9-2. Provide additional descriptive information regarding supply chain risk or security awareness training provided

10-1. Is your organization employing proper access controls for the protection of product-relevant intellectual property? Examples include employee background checks, privileged access (role or rule-based) access control measures, physical boundary control measures, and separation and rotation of duties.

○ Yes-Fully
○ Yes-Partially
○ No

10-2. Provide additional descriptive information on access controls utilized for protection of product-relevant intellectual property

11-1. Do you internally manufacture all Printed Circuit Board Assembly (PCBA) subsystems for your products, specifically Main PCBAs, like motherboards?

○ Yes-Fully
○ Yes-Partially
○ No

11-2. Provide any additional descriptive information on the internal manufacturing of PCBA subsystems

□

11-3. If the response to Question 11-1 is No, do you employ a Risk Management Framework (RMF) or similar process to assess your PCBA suppliers' capability to protect their manufacturing baselines and reduce the likelihood of counterfeit or contaminated components being introduced during the manufacturing process?

○ Yes-Fully
○ Yes-Partially
○ No

11-4. Provide additional descriptive information on your organization's Risk Management Framework (RMF) or similar process

□

12-1. Do you use redundant suppliers for PCB Production, Assembly Production and Test Subsystem design?

○ Yes-Fully
○ Yes-Partially
○ No

12-2. Provide additional descriptive information on how redundant suppliers are utilized

□

13-1. Are the test systems hardware used to validate and certify manufactured components also under your company's Configuration Management (CM) control?

○ Yes-Fully
○ Yes-Partially

○ No

13-2. Provide additional descriptive information on how your organization ensures the test systems hardware are under your organization’s Configuration Management (CM) control

□

14-1. Are the test systems software and firmware used to validate and certify manufactured components also under Configuration Management (CM) control?

○ Yes-Fully
○ Yes-Partially
○ No

14-2. Provide additional descriptive information on which test systems software are under your organization’s Configuration Management (CM) control

□

15-1. Does your organization use Open Source or 3rd party software or code to build your products or services?

○ Yes-Fully
○ Yes-Partially
○ No

15-2. Provide additional descriptive information on Open Source or 3rd party software or code used to build your products or services

□

15-3. If the response to Question 15-1 is Yes (Fully or Partially), are the Open Source or 3rd party software or code used in the development of your products warrantied or supported for vulnerability updates?

○ Yes-Fully
○ Yes-Partially
○ No

15-4. Provide additional descriptive information on what warranties or support are provided for vulnerability updates

□

16-1. Do you employ static and/or dynamic testing of your software or firmware source code?

○ Yes-Fully
○ Yes-Partially
○ No

16-2. Provide additional descriptive information on the static and/or dynamic testing of your software or firmware source code

□