CYBER SUPPLY CHAIN RISK MANAGEMENT QUESTIONNAIRE
Table of Contents

1 Introduction 3
2 Form Questions 4
3 Form Submission 10
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]. The following is an abstract of that 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 multiteried, SCRM-specific approach, including guidance on supply chain risk assessment and mitigation activities."

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 Questions

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

- Yes-Fully
- Yes-Partially
- No

1-2. Provide any additional descriptive information

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 any additional descriptive information

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 any additional descriptive information

2-3. Does your organization employ techniques and practices for conducting vulnerability assessments on your products software, firmware and/or hardware components?
3-2. Provide any additional descriptive information


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

☐ Yes-Fully
☐ Yes-Partially
☐ No

4-2. Provide any additional descriptive information


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 any additional descriptive information


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 any additional descriptive information
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 any additional descriptive information

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

- Yes-Fully
- Yes-Partially
- No

6-4. Provide any additional descriptive information

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 any additional descriptive information

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 any additional descriptive information

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 any additional descriptive information

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 any additional descriptive information

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
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 any additional descriptive information


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

- Yes-Fully
- Yes-Partially
- No

12-2. Provide any additional descriptive information


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 any additional descriptive information


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 any additional descriptive information

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 any additional descriptive information

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 any additional descriptive information

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 any additional descriptive information

Page : 9
Form Submission

First Name:

Last Name:

Job Title:

Email Address: