

CYBER-SUPPLY CHAIN RISK MANAGEMENT PLAN

Version 1 - 4/2/24

INSTRUCTIONS

INTRODUCTION:

U S adversaries have attacked our nation's supply chains and compromised Federal Government systems, capitalizing on security weaknesses in U S companies and third party affiliates. It is incumbent on NASA SEWP's industrial base to implement vigilant Supply Chain Risk Management procedures to ensure proper risks and mitigation of risks are identified.

This document is intended to evaluate a potential contractor's SCRM maturity.

TEMPLATE COMPLETION INSTRUCTIONS:

- Provide a contact (name, email, and phone number) for questions, support, or additional information related to the questionnaire to the respondents.
- 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 information technology, acquisition, procurement, supply chain, or security offices. While related, each section is designed 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.
- Provide your responses in the text box in the text entry boxes provided.
- Provide a response to each 'Yes', 'No' question as relevant to the offering.
- If the response is No, provide a summary explanation and risk mitigation plan in the summary explanation box.

If the requested supply chain risk management information on the next tab has previously been provided to the requesting organization, provide an updated revision covering material changes.

A Critical Component is defined as: A system element that, if compromised, damaged, or failed, could cause a mission or business failure.

C-SCRM PLAN TEMPLATE

CONTACT INFORMATION

Name of Respondent:

Title:

Name of Organization:

Phone number:

Email:

SECT. 1	SUPPLY CHAIN PROVENANCE	VENDOR RESPONSE (Yes/No)	If the response is No, provide a summary explanation and risk mitigation plan
	Identity - including that of each parent and/or subsidiary corporate entities.		
1.1	Are suppliers of critical ICT components identified?		
1.2	Is the company ownership of suppliers of critical ICT components verified?		
1.3	Are suppliers of critical ICT components under U.S. ownership?		
1.4	If distributors will be used to provide products/services to the Government, is a threat analysis performed for each distributor?		
1.5	Are any subcontractors and/or suppliers located outside the United States or its territories? If "yes", list company name(s) and foreign country location(s).		
1.6	Are Basic Security Requirements (not Derived Security Requirements) implemented for the fourteen families in Chapter Three of NIST SP 800-171 R3, Protecting Controlled Unclassified Information in Nonfederal Systems?		
SECT. 2	SUPPLY CHAIN MANAGEMENT AND SUPPLIER GOVERNANCE		
	General		
2.1	Are policies/processes in place to ensure timely notification of updated risk management information previously provided to the Contracting Officer and Contracting Officer's		
	Information Communications Technology (ICT) Supply Chain Management		
2.2	Is there a documented Quality Management System (QMS) based on an industry standard or framework for the prime contractor's Information and Communications Technology (ICT) supply chain operation? If "yes" provide QMS documentation.		
	Supplier Governance		
2.3	Do Supply Chain Risk Management (SCRM) requirements exist in contracts with critical ICT		
2.4	Is there a process to verify that suppliers are meeting SCRM contractual terms and conditions, including, where applicable, requirements to be passed down to sub-suppliers?		
SECT. 3	INFORMATION SECURITY		
	Identify		
3.1	Is there a process used to verify that information is categorized according to legal, regulatory, or internal sensitivity requirements?		
3.2	Are the policies and procedures referenced in 3.1 reviewed and updated annually? When was the most recent review?		
	Detect		
3.3	Are incident detection and reporting practices defined and documented which outline the actions that should be taken in the case of an information security or cybersecurity event?		
3.4	Are cybersecurity events centrally logged, tracked, and continuously monitored?		
3.5	Is endpoint protection software deployed throughout the prime contractor's environment? If "no", describe the mitigation efforts used instead.		
3.6	Is there a documented incident response process and a dedicated incident response team (CSIRT - Computer Security Incident Response Team)? If "no", describe the mitigation efforts used instead.		
SECT. 4	PHYSICAL SECURITY		
	General		
4.1	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		
4.2	Are security policies and procedures documented which address the control of physical access to cyber assets (network devices, data facilities, patch panels, industrial control systems, programmable logic, etc.)?		
4.3	Are physical security industry standards/controls adhered to? (e.g., NIST publication, ISO, UL, etc.)		

4.4	Are the policies and procedures listed in 4.3 reviewed and updated at least annually? When was the most recent review?	
4.5	Does a documented Security Incident Response process exist which covers physical security incidents at the prime contractor's owned or operated facilities (e.g., potential intruder access, missing equipment, etc.)? If "no", describe mitigation efforts.	
Physical Security In-transit		
4.6	Are requirements in place to ensure the use of Original Equipment Manufacturer (OEM) or Authorized Distributors for all critical ICT components?	
4.7	Are counterfeit prevention requirements passed on to second and third party suppliers?	
SECT. 5 PERSONNEL SECURITY		
General		
5.1	Is a personnel security program implemented at the prime contractor's owned or operated	
5.2	Are physical security practices documented or formally governed?	
Onboarding		
5.3	Are policies documented for conducting background checks of prime contractor employees as permitted by each country in which you operate?	
SECT. 6 SUPPLY CHAIN INTEGRITY		
General		
6.1	Are documented processes in place for managing third-party products and component defects throughout their lifecycle?	
6.2	What provisions for auditing are included within supplier contracts?	
6.3	Are hardware/software products or services integrity and End of Life requirements passed down to second and third party suppliers?	
6.4	Are processes in place for addressing reuse and/or recycle of hardware products?	
SECT. 7 SUPPLY CHAIN RESILIENCE		
General		
7.1	Is a formal process documented for ensuring supply chain resilience as part of your product offering SCRM practices?	
Supply Chain Disruption Risk Management (Business Continuity)		
7.2	Can prime contractor personnel work remotely?	
7.3	Is a data backup policy in place that aligns with NIST SP 800-53 CP-9?	
7.4	Has your organization conducted vulnerability assessments, risk assessment, or other calculations to identify what impact physical risks associated with climate related risks (e.g., increases in precipitation-driven flooding, extreme heat events, and inundation due to sea level rise and storm surge) might have on your assets, products, and/or services?	
7.6	Does your organization have a disaster response plan that includes contingency plans and response protocols for potential short-term acute events (e.g., hurricane, earthquake, flooding, and etc.) and long-term climate related risks impact (e.g.; changes in precipitation, increased average temperature, and sea level rise)?	
7.7	Does your organization's disaster response plan include how to manage potential increases in frequency, severity, or duration of weather events?	
7.8	Does the disaster response plan describe which assets, products, services would most significantly disrupt operations if they experienced short term acute damage (immediate failure, either temporary or catastrophic).	
7.9	Does the disaster response plan describe which assets, products, services, would most significantly disrupt operations if they experienced gradual long-term cumulative damage (slower degradation; greater wear and tear).	