ATTACHMENT J.P-17
A3 C-SCRM (CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT) PLAN PREPARATION GUIDE

Purpose: The Attachment J.P-17 Alliant 3 C-SCRM (Cybersecurity Supply Chain Risk Management) Plan Preparation Guide is provided to prospective offerors to ensure a standardized approach to identifying, assessing, and mitigating risks within the cybersecurity supply chain. As outlined in Section L.5.5.2 the preparation guide serves several key purposes:

- Guidance and Standardization: It offers detailed instructions and criteria for the development of a comprehensive C-SCRM plan. This ensures that all offerors are aligned with the expectations and requirements, promoting a uniform understanding and approach to cybersecurity supply chain risk management across all proposals.
- Risk Management: By adhering to the guide, offerors are equipped to effectively identify potential cybersecurity threats and vulnerabilities within their supply chains. It enables them to develop and implement strategies that mitigate these risks, ensuring the security and integrity of their products and services.
- Compliance: The guide ensures that all proposals meet the regulatory and contractual requirements related to cybersecurity and supply chain risk management. This compliance is critical for both the protection of national security interests and the establishment of trust in the capabilities of the offerors to manage complex cybersecurity challenges.
- Evaluation Consistency: By providing a standardized framework for the preparation of the C-SCRM plan, the guide facilitates a more efficient and consistent evaluation process. This allows evaluators to effectively assess the adequacy and effectiveness of each offeror's plan against a common set of criteria, ensuring a fair and competitive selection process.
- Enhancement of Cybersecurity Posture: Ultimately, the guide is designed to enhance the overall cybersecurity posture of the supply chain. By preparing a robust C-SCRM plan, offerors demonstrate their commitment to safeguarding against cyber threats, contributing to a more secure and resilient supply chain environment.

The Attachment J.P-17 Alliant 3 C-SCRM Plan Preparation Guide is a critical resource for prospective offerors, guiding them in the creation of effective and compliant cybersecurity supply chain risk management plans. Through adherence to the guidelines provided in Section L.5.5.2 offerors can ensure their proposals meet the highest standards of security, compliance, and risk management, thereby supporting the goal of securing the supply chain against evolving cyber threats.

Cybersecurity Supply Chain Risk Management (C-SCRM) Plan Preparation Guide

Version 1.00

March 2023

This page is intentionally left blank.

REVIEW LOG

Date of Review	Reviewer	Organization

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. REVISIONS AND MAINTENANCE INSTRUCTIONS

A document change control and review log table are provided in the C-SCRM Plan on page ii and iii. Organizations must identify the document version number, date of the review, a summary of the changes, the section or pages which contain the changes, and the name of the individual who made the change. At a minimum, review and update the C-SCRM Plan annually, and in conjunction with life cycle milestones, gate reviews, and significant contracting activities. Then, verify it for compliance with upper tier plans as appropriate. Ensure the plan adapts to shifting impacts of exogenous factors, such as threats, enterprise, and environmental changes.

- **Instructional Note:** Remove the red font instructional text row for document submission.
- **Numbering Convention for Document Change Control Table:** Version | Revision as V.R.R. Pre-publication drafts are 0.xx; first published version is 1.00; for minor revisions to a published document, increment the decimal number (e.g., 1.01) for major content upgrades to a published document, increment the leading whole number (ex., 2.00). Update the version field on the top right of the header to match the latest version listed below.

DOCUMENT CHANGE CONTROL				
	Release Date	**Summary of Changes**	**Section / Pages Affected**	**Author**
1.0	*1/10/2023*	*Added Additional Roles*	*Section 9*	*Stu Pendous*
1.1	*2/20/2023*	*Updated Operational Status*	*Section 5*	*Fran Tastic*

Figure 1 - Document Change Control Example

REVIEW LOG		
Date of Review	**Reviewer**	**Organization**
1/10/2023	*Stu Pendous*	*ACME*
2/20/2023	*Fran Tastic*	*ACME*

Figure 2 - Review Log Example

2. DOCUMENT GUIDANCE

The guidance is provided to assist organizations in preparing the C-SCRM Plan for an acquirer review. Once completed, the C-SCRM Plan provides detailed descriptions of: (1) All system control implementations; (2) The system's purpose, function, and operations, including inventories of its components and services; and (3) Detailed depictions of the system's data flow, architecture, and authorization boundary.

2.1. INSTRUCTIONS

2.1.1. Standard Language

The C-SCRM Plan template includes standard language provided as explanations of common procedures. Standard language is ***not to be changed*** or modified.

2.1.2. Sample Language

This template includes sample language in **blue** font and is provided as a placeholder to assist the author in creating standard document language by providing a guide as to the context of what should be written. This language can be ***reviewed*** and ***modified/replaced*** by the author to be system-specific. Prior to document submission, change the color of text to **black** to match the paragraph text. **NOTE:** The *light blue italicized* font in Section 11, C-SCRM Security Control Details, is not Sample Language; it identifies specific General Services Administration (GSA) organization-defined parameters (ODPs) and should not be changed.

2.1.3. Red Bracketed Text

This template includes placeholder text surrounded by brackets (i.e., [Text]). To personalize the document, the author ***must*** replace the placeholder text with system relevant text, then change the color of text to black to match the paragraph text.

2.1.4. Content Controls

This template includes drop-down list content controls to assist the author in selecting one of preset values from pull-down menu. The author must choose the preferred option.

2.1.5. Call-Out Boxes

Call-out boxes are graphical design elements used in this template to call attention to important information. The two (2) types of call-out boxes used in this document are explained below.

Red call-out boxes are instructions for completing each section. Once the section is completed, the red call-out boxes are to be deleted.

Gray call-out boxes are important items to note. This language can be used as-is, modified, replaced, or removed by the author.

3. SYSTEM NAME AND IDENTIFIER

The Cybersecurity Supply Chain Risk Management (C-SCRM) Plan begins with listing the name and identifier of the system. Each system should be assigned a unique name and identifier to help ensure appropriate security requirements are met based on the unique requirements for the system, and allocated resources are appropriately applied. Further, the use of unique system identifiers is integral to the Information Technology (IT) system investment models and analyses established under the requirements of the Federal Information Security Modernization Act (FISMA) and the Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act). The identifier could be a combination of alphabetic and numeric characters and can be used in combination with the system name or could be the acronym of the system name. The unique name and identifier should remain the same throughout the life of the system to allow the organization to track completion of security requirements over time.

Table 1 System Name and Identifier	
System Name	A Company that Makes Everything
Unique Identifier	ACME

Figure 3 - System Name and Identifier Example

C-SCRM security controls may apply to different participants of the supply chain. Each system must identify its organization's offering type and provider type below to set expectations for the auditor's review as per National Institute of Standards and Technology (NIST) Special Publication (SP) 800-161 Rev. 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, Appendix A: C-SCRM Security Controls, Applying C-SCRM Controls to Acquiring Products and Services.

Table 2 Offering and Provider Type	
Offering Type	Service
Provider Type	External System Service Provider of Information System Services

Figure 4 - Offering and Provider Type Example

4. SYSTEM DESCRIPTION

The system description must describe the function, purpose, and scope of the system; and include a description of the information which is processed. Provide a general description of the system's approach to managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the system, system components, or system services.

Ensure the C-SCRM Plan describes the system in the context of the enterprise's supply chain risk tolerance, acceptable supply chain risk mitigation strategies or controls, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the plan, and a description of and justification for supply chain risk mitigation measures taken. Descriptions must be consistent with the high-level mission/business function of the system, the authorization boundary of the system, overall system architecture, including any supporting systems and relationships, how the system supports enterprise missions, and the system environment (e.g., standalone, managed/enterprise, custom/specialized security-limited functionality, cloud) established in Level 1 (Enterprise) and Level 2 (Mission/Business Processes).

If the system is a general support system, list all applications supported by the general support system. Specify if the application is or is not a major application and include unique name/identifiers, where applicable. Describe each application's function and the information processed. Include a list of user organizations, whether they are internal or external to the system owner's organization, and a general description of the type of information and processing provided.

The Globe-X Document Management System (DMS) serves to provide dynamic information repositories, file hierarchies, and collaboration functionality to streamline internal team communication and coordination. The data managed within the system contains personally identifiable information (PII). The DMS is a commercial off-the-shelf (COTS) solution that was purchased directly from a verified supplier ACME within the United States. It has been functionally configured to meet the enterprise's needs; no third-party code libraries are utilized to deploy or maintain the system. It is hosted within the management layer of the enterprise's primary virtual private cloud provider.

The DMS is a Category 1 system, mandating a recovery time objective (RTO) of one hour in the event of downtime. The enterprise maintains a disaster recovery environment with a second private cloud provider to which the enterprise can cutover if the Category 1 RTO is not likely to be met on the primary platform.

Figure 5 - System Description Example

5. SYSTEM INFORMATION TYPE AND CATEGORIZATION

The following table specifies the information types processed, stored, or transmitted by the system and/or its in-boundary supply chain. Enterprises utilize NIST SP 800-60 Rev. 1, Volume II, *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*, to identify information types and provisional impact levels. Using guidance regarding the categorization of federal information and systems in NIST Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, the enterprise determines the security impact levels for each information type. For each security objective (i.e., confidentiality, integrity, availability), the impact level (i.e., low, moderate, high) must be identified.

Instructions on How to Edit the Embedded Excel Worksheet (Figure 4 - System Security Categorization):

To dramatically reduce the time and effort needed to categorize information and system type impact levels, the following automated and rule-based categorization tool is provided.

1. To edit the content of an embedded Excel worksheet in Word, return to editing mode:
    a. Double-click the embedded Excel worksheet object in the document to open Excel.
    b. Select the necessary FIPS 199 information types in Column 1 via the drop-down list.
    c. Once all information types are selected, click **CTRL** + **HOME** to move the cursor to the title cell.
2. To change the Excel worksheet back into an embedded table in Word when finished, click the "**X**" on the upper right-hand corner to close Excel, then click back into the Word document.

System Security Categorization

Overall System Security Category			Confidentiality	Integrity	Availability
Moderate			Low	Moderate	Low
FIPS 199 Information Type Catalog			Impact Level		
FIPS 199 Information Type	Business Line	Business Area	Confidentiality	Integrity	Availability
Inventory Control	Management of Government	C.3.4 Supply Chain Management	Low	Low	Low
Information Security	Management of Government	C.3.5 Information & Technology	Low	Moderate	Low
Corrective Action (Policy/Regulation)	Support Delivery of Services	C.2.1Controls and Oversight	Low	Low	Low
Services Acquisition	Management of Government	C.3.4 Supply Chain Management	Low	Low	Low

Figure 6 - System Security Categorization Example

6. REVISIONS AND MAINTENANCE

This section defines the frequency requirement to review and update the strategy and implementation document. Specifically, the plan is a living document and should not have an expiration date.

7. SYSTEM OPERATIONAL STATUS

In Table 3, System Operational Status, indicate one or more of the following for the system's operational status via the drop-down list. If more than one status is selected, list which part of the system is covered under each status in the explanation row.

- **Operational** - The system is currently operating and is in production.
- **Under Development** - The system is being designed, developed, or implemented.
- **Major Modification** - The system is undergoing a major change, development, or transition.
- **Disposition** - The system is no longer operational.

If the system is under development or undergoing a major modification, provide information about the methods used to assure that up-front security requirements are included. Include specific controls in the appropriate sections of the plan depending on where the system is in the security life cycle.

Table 3 System Operational Status	
Status One	Operational - The system is currently operating and is in production.
Status Two (Optional)	Not Applicable (N/A)
Explanation	The system currently has only one operational status.

Figure 7 - System Operational Status Example

8. SYSTEM ENVIRONMENT

8.1. Operational Environment Type

Each system must identify its organization's operational environment type. Identifying the operational environment allows auditors to set expectations and target their review to the security requirements associated with the selected environment. Complete Table 4, Operational Environment Type, by selecting the "Type" from the drop-down menu and provide the Custom/Other Explanation details as needed. The typical environment types are:

- **Standalone or Small Office/Home Office (SOHO)** describes small, informal computer installations that are used for home or business purposes. Standalone encompasses a variety of small-scale environments and devices, ranging from laptops, mobile devices, or

home computers, to telecommuting systems, to small businesses and small branch offices of a company.

- **Managed or Enterprise** are typically large agency systems with defined, organized suites of hardware and software configurations, usually consisting of centrally managed workstations and servers protected from the Internet by firewalls and other network security devices.
- **Custom** environments contain systems in which the functionality and degree of security do not fit the other environments. Two typical Custom environments are Specialized Security-Limited Functionality and Legacy:
  - **Specialized Security-Limited Functionality**. A Specialized Security-Limited Functionality environment contains systems and networks at high risk of attack or data exposure, with security taking precedence over functionality. It assumes systems have limited or specialized (not general-purpose workstations or systems) functionality in a highly threatened environment such as an outward-facing firewall or public web server or whose data content or mission purpose is of such value that aggressive trade-offs in favor of security outweigh the potential negative consequences to other useful system attributes such as legacy applications or interoperability with other systems. A Specialized Security-Limited Functionality environment could be a subset of another environment.
  - **Legacy**. A Legacy environment contains older systems or applications that may use older, less-secure communication mechanisms. Other machines operating in a Legacy environment may need less restrictive security settings to communicate with legacy systems and applications. A Legacy environment could be a subset of a standalone or managed environment.

Table 4 Operational Environment Type	
Type	Managed or Enterprise
Custom\Other Explanation	Not Applicable (N/A)

Figure 8 - Operational Environment Type Example

8.2. Network Diagrams

The detailed architecture diagram(s) illustrate(s) the design and implementation of a system or network. In accordance with NIST SP 800-37 Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, the architecture diagram(s) must clearly show the authorization boundary and all system elements to be tested, all of which "the organization agrees to protect under its direct management or within the scope of its responsibilities."

The detailed architecture diagram(s) must clearly show the authorization boundary and all of the systems elements to be tested.

Detailed architecture diagram(s) must, at a minimum:

- Have a border
- Have a title and description (e.g., Information System (IS) Name - Detailed Architecture Diagram)
- Include the city and state where the components are located (e.g., Arlington, VA)
- Have a revision date (e.g., 22 April 2022)
- Have a version number (e.g., v1.00)
- Have a legend or key that must be legible
- Clearly delineate accreditation boundaries with a red dotted line
- Identify any connections to any internal and external systems, networks, and/or enclaves
    - Identification of internal and external connected enclaves must include:
        - The name of the organization that owns the enclave
        - The connection type (e.g., wireless, dedicated point-to-point, etc.)
        - Internet protocol (IP) addresses and subnet mask for all devices within the enclave
        - The organization type (e.g., GSA, Federal agency, contractor, etc.)
- Depict the interconnected ISs for any documented Interconnection Security Agreement (ISA), Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA), or Service Level Agreement (SLA)
- Show (if applicable) other connections (access points); the flow of information to, from, and through all connections; and host IP addresses, if known must be shown
- Depict internal and external traffic. Differentiate the two by color and direction; unidirectional or bidirectional.

Network zones must:

- Be grouped using containers
- Identify Demilitarized Zone (DMZ) for publicly accessible devices
- Identify Test, Development, Pre-Production, and Production Zones

Detailed architecture diagram components must:

- Include the host name (e.g., FLT-ARO1)
- Include device type (e.g., Access Router)

- Include the model number (e.g., Cisco 871)
- Include the IP address (e.g., 10.255.255.15/8 or XXX.XXX.255.15/8)
- Show actual and planned interfaces to internal and external local area networks (LANs) or wide area networks (WANs) (including backside connections)
- Identify equipment inventory (to include the most recent configuration and any enclave boundary firewalls, intrusion detection systems (IDSs), premise routers, routers, switches, backside connections, IP addresses, encryption devices, cross domain solutions (CDS)
- Group items using containers
- Identify any other Information Assurance (IA) or IA-enabled products deployed in the enclave
- Identify the Internetwork Operating System (IOS) version
- For each hardware component shown on the diagram, include an IP address and host name (traceable to the hardware inventory list)
- For each server component shown on the diagram, include the type of server (e.g., database, web, file, etc.)
- Include workstation subnets - Can be represented using a range of IP addresses; icons for individual workstations are not required
- Include printer subnets - Can be represented using a range of IP addresses; icons for individual printers are not required
- Clearly identify perimeter devices within the authorization boundary that control inbound and outbound access
- Clearly identify components within the authorization boundary supporting remote access must
- Clearly identify wireless devices (if any) within the authorization boundary
- Include representation of all components with IP addresses
    - The IP addresses on the detailed architecture diagram should be traceable to the hardware inventory and the IP addresses on the hardware inventory should be traceable to the diagram
- Identify interface names as needed for clarification
- Identify hardware location

Connections must be labeled to:

- Identify connection type (e.g., virtual private network [VPN], Multiprotocol Label Switching [MPLS] cloud, dedicated point-to-point)
- Identify link type (e.g., fiber-optic link, copper link, wireless access point)

- Identify network layer information (e.g., Layer 1 [L1], Layer 2 [L2], Layer 3 [L3])
- Identify line speed (e.g., 1GB, 100Mb, 10Mb)
- Identify Ports, Protocols, and Services (e.g., Transmission Control Protocol [TCP] 80, TCP 443, User Datagram Protocol [UDP] 67)
- Identify VLAN ID information (e.g., 200, 300,400)
- Identify encryption types (e.g., Internet Protocol Security [IPsec], Secure Sockets Layer [SSL], Transport Layer Security [TLS])
- Identify in-band and out-of-band management

8.3. System Component Inventory

OMB Circular A-130, "Management of Federal Information Resources," and 44 U.S.C. 3511, Establishment and operation of Government Information Locator Service, require all U.S. Federal agencies to maintain hardware, software, and firmware inventories for their systems. Vendors may utilize the provided Attachment 1 - System Component Inventory to document an inventory of system hardware, software, and operating system components that:

- Accurately reflects the current system and is readily available
- Includes all components within the authorization boundary of the system
- Is at the level of granularity deemed necessary for tracking and reporting
- Includes hardware inventory specifications: Device Type, Device Role, DNS Name, IP Address, Logical Location, Physical Location, Manufacturer, Model, Serial Number, etc.
- Includes software inventory specifications: Software Type, Vendor Name, Application Name, Version, License Type, Platform Installed, etc.

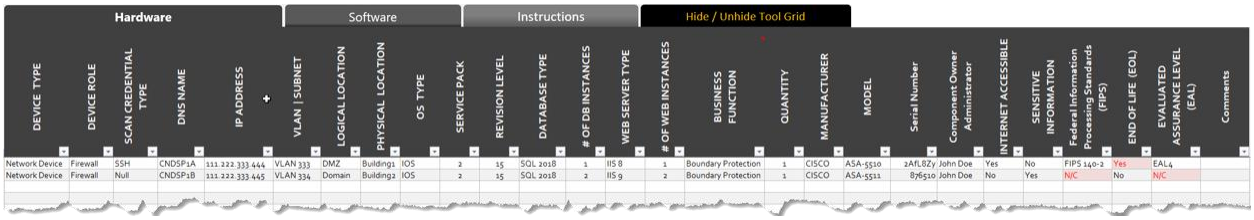

Figure 9 - Hardware Inventory Example

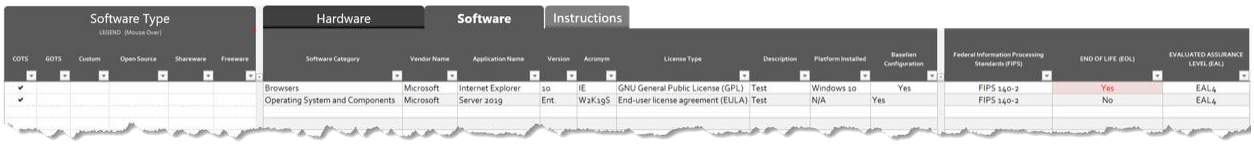

Figure 10 - Software Inventory Example

9. INFORMATION EXCHANGE AND SYSTEM CONNECTIONS

System interconnection is the direct connection of systems for the purpose of exchanging information resources (data or services). System interconnection, if not appropriately protected, may result in a compromise of all connected systems and the data they store, process, or transmit. It is important that system operators, information owners, and management obtain as much information as possible about the vulnerabilities associated with system interconnection, information sharing, and the increased controls required to mitigate those vulnerabilities. The C-SCRM Plan for the systems often serves as a mechanism to affect this security information exchange and allows management to make informed decisions regarding risk reduction and acceptance.

OMB Circular A-130 requires written management authorization (often in the form of an ISA, MOU, and/or MOA) be obtained prior to connecting with other systems and/or sharing sensitive data/information. The written authorization shall detail the rules of behavior and controls that must be maintained by the interconnecting systems.

In this section, provide the following information concerning the authorization for the connection to other systems or the sharing of information.

Table 5 documents high-level information for all system interconnections. List all interconnected systems in the table below and add rows as needed. If an ISA/MOU/MOA is not required, place "N/A" in both the Agreement Date and Agreement Type columns.

A system interconnection is the direct connection of two or more systems for the purpose of sharing information resources (data or services). An ISA, MOU, or MOA is required between systems that share data which is owned or operated by different organizations and where data is transmitted between each system. All interconnections between the system and external entities including off-site contractors or Federal agency/departments must be approved by the Authorization Official (AO).

List the date of the agreement, any information exchange agreements between the system and another system, the enterprise or organization's name that owns the other system, the system's FIPS 199 categorization, security authorization status of the other system(s), the name of the authorizing official, and type of connection or information exchange.

Table 5 System Interconnections

Agreement Date	Agreement Type	Name of System	Enterprise or Organization Name	Type of Connection or Information Exchange	FIPS 199 Categorization	Authorization Status	Authorization Official Name and Title
6/1/2022	ISA	Techizar	Amazon Web Services (AWS)	IPsec site-to-site VPN	High	Authorization to Operate	Fran Tastic Authorizing Official (AO)

Table 5 System Interconnections							
Agreement Date	Agreement Type	Name of System	Enterprise or Organization Name	Type of Connection or Information Exchange	FIPS 199 Categorization	Authorization Status	Authorization Official Name and Title
7/4/2022	MOA	Mobiacom	Microsoft Azure	Dynamic Multipoint (DMVPN)	Moderate	Authorization to Operate	Mike Roscopic Authorizing Official (AO)
1/2/2022	MOU	Telcella	Google Cloud	MPLS-based L3VPN	Low	Authorization to Use	Stu Pendous Authorizing Official (AO)

10. CONTINGENCIES AND EMERGENCIES (OPTIONAL)

For organizations that choose to complete this section in the event of contingency or emergency operations, enterprises may need to bypass the normal C-SCRM acquisition processes to allow for mission continuity. Contracting activities that are not vetted using approved C-SCRM plan processes introduce operational risks to the enterprise.

Where appropriate, describe abbreviated acquisition procedures to follow during contingencies and emergencies, such as the contact information for C-SCRM, acquisitions, and legal subject matter experts who can provide advice absent a formal tasking and approval chain of command.

Complete Table 6, Contingency and Emergency Contacts, with the current contact information for C-SCRM subject matter experts (SMEs) as shown in the example, Figure 11, Contingency and Emergency Contacts Example.

Table 6 Contingency and Emergency Contacts			
Point of Contact (POC)	Name	E mail Address	Phone Number
C-SCRM SME POC	Fran Tastic	Fran.Tastic@acme.com	(202) 555-0174
Acquisitions SME POC	Mike Roscopic	Mike.Roscopic@acme.com	(202) 555-0260
Legal SME POC	Stu Pendous	Stu.Pendous@acme.com	(202) 555-0145

Figure 11 - Contingency and Emergency Contacts Example

11. APPLICABLE LAWS AND REGULATIONS

Nothing needs to be done to this section. See Appendix B, Related Laws and Regulations, to add or remove any applicable laws and regulations.

12. ROLES AND RESPONSIBILITIES

Identify the roles and responsibilities of key cybersecurity supply chain personnel or designate contacts (e.g., vendor contacts, acquisitions SMEs, engineering leads, business partners, and service providers) by risk management level in the provided table. Boilerplate roles and responsibilities (in black text) have been provided for C-SCRM standard roles. Red font

placeholders have been provided to add roles and responsibilities. Add or remove rows, as necessary.

There are several roles, sometimes referred to as positions or functions, defined in the RMF that help ensure successful implementation. For each task, designated roles are assigned primary responsibility and supporting responsibility. While the primary role is accountable for the task, unless specifically prohibited, tasks can be delegated. To ensure clear designation, roles should be assigned to align with signed appointment letters. The roles and associated responsibilities must be relevant to the activities in this C-SCRM Plan, and some may be in addition to the roles and responsibilities defined in NIST SP 800-161 Rev. 1, Section 2.3.1, Roles and Responsibilities Across the Three Levels; and NIST SP 800-37 Rev. 2, Appendix D, Roles, and Responsibilities.

13. C-SCRM CONTROL DETAILS

DISCLAIMER OF ENDORSEMENT. Reference to any specific product, service, process, or method by trade name, trademark, service mark, manufacturer or otherwise in this section does not constitute an implied or expressed recommendation or endorsement, or favoring by the General Services Administration, its employees, officers, employees, or contractors.

Any specific product name mentioned in this document is used for instructional purposes only, to demonstrate the type of technology that could be used when addressing the specific security requirements of a control.

This section provides guidance on the process of accurately documenting control implementation statements for the system and environment of operation described in the C-SCRM Plan.

The C-SCRM control baseline has a total of 40 controls requiring written implementation statements.

There are a total of 294 applicable controls documented in NIST SP 800-161 Rev. 1. As part of the Program, vendors are responsible for documenting control implementations for 40 controls. At the task order level, vendors may be responsible for documenting additional controls.

The purpose of control implementation statements is to provide an overview of the actual implementation of each selected control in the context of a specific system with a sufficient level of detail to correctly implement the control and to subsequently assess the effectiveness of the control as implemented in the system.

The process of documenting the implementation of controls carries significant risk management implications and is therefore an organization-wide activity which requires coordination among key participants. The System Owner (SO) is responsible for documenting the controls for the system and environment of operation in C-SCRM Plans. The SO may also coordinate/delegate control documentation activities to the following supporting roles: Information Owner or Steward;

Systems Security Engineer; Privacy Engineer; System Security Officer; and System Privacy Officer.

The control implementation structure consists of well-defined components relevant to control implementation and:

- Provides an overview of the security, privacy, or C-SCRM requirements for the system.
- Outlines predefined assignment and selection statements (also called control parameters or organization-defined parameters).
- Provides a status of the controls implemented or planned for meeting security, privacy, and C-SCRM requirements.
- Defines the scope of applicability for the control.
- Facilitates documentation of effective application of controls to achieve adequate information security.
- Establishes appropriate expectations for systems protection.

The figure below illustrates the structure of the eight (8) components of a typical control implementation statement.

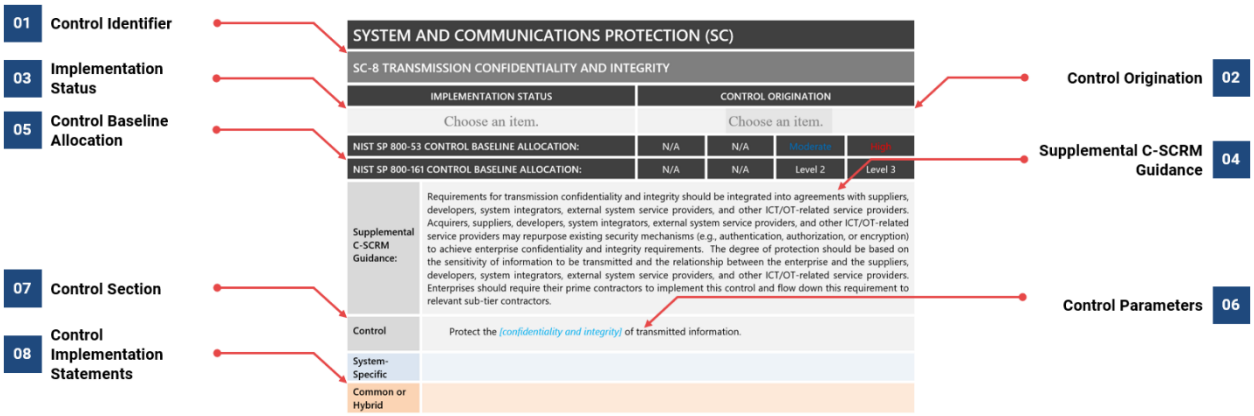

Figure 12 - Typical Control Implementation Structure

While the above provides the recommended format for describing how a control is implemented, the implementation statement can alternatively be written in paragraph form. If this option is taken, the response must include the following elements:

- Control Identifier
- Control Origination
- Implementation Status
- Supplemental C-SCRM Guidance
- Control Parameters
- Control Implementation Statement

Note the control implementation statement must speak to all elements of the Control Parameters, which should be easily identifiable in the response; and specifically note any parts of the implementation which are common or hybrid versus system specific.

13.1. Component 1 of 8: Control Identifier

The Control Identifier provides a standard representation and description for each of the singular, actionable measurable statements that comprise a control.

- The two-character identifier uniquely identifies each control family (e.g., AC for Access Control).
- The control number indicates the controls sequentially numbered within each family (e.g., AC-1, AC-2, etc.).
- The bracketed numbers following the control number represent a control enhancement, which provides additional protection in the same general subject area as the control to which they "belong" (e.g., AC-2(3)).
- The control description notes the high-level title of the control (e.g., AC-2, Account Management).
- Each control enhancement has a short subtitle to indicate the intended function or capability provided by the enhancement (e.g., AC-2(3), Account Management | Disable Inactive Accounts).

It is important to note that control enhancements are treated as if they are simply additional security controls.

13.2. Component 2 of 8: Control Origination

The Control Origination defines the responsible party for the control's implementation. There are three (3) distinct types of control originations: Common Control, System-Specific Control, and Hybrid Control.

- The control origination defines the scope of applicability for the control; the shared nature or inheritability of the control; and the responsibility for control development, implementation, assessment, and authorization.
- The origination of control has a specific focus and objective which helps organizations implement the controls effectively and obtain the expected protection benefits.
- Deploying certain types of controls (e.g., common controls) may also achieve cost benefits by leveraging security, privacy, and C-SCRM capabilities across many systems and environments of operation.
- **Common Controls** are controls whose implementation results in a capability inheritable by multiple systems or programs.

- **System-Specific Controls** are controls whose implementation is the primary responsibility of the SO and authorizing officials (if applicable) for a system.
- **Hybrid Controls** are controls implemented in a system in part as a common control and in part as a system-specific control.

13.3. Component 3 of 8: Implementation Status

The Implementation Status is the standing of a control implementation to meet a set of defined security requirements. The control implementation status defines the application and functionality of the control. There are three (3) distinct types of control implementation statuses. These include Implemented Control, Planned Control, and Not Applicable Controls.

- **Implemented Controls** are controls fully implemented and functioning as intended.
- **Planned Controls** are controls not fully implemented and functioning as intended.
- **Not Applicable Controls** are controls determined not to apply or are incapable of being applied to a system.
  - It is very rare to have a control with an implementation status of Not Applicable. For example, if a system does not have wireless access (AC-18), the control implementation status should not be marked as Not Applicable. The organization should mark the control as Implemented and explain; for example, the organization's implementation of a wireless access restriction policy as well as a Wireless Intrusion Prevention System (WIPS) for detection of rogue Wi-Fi devices within the authorization boundary.
  - The SO should read the supplemental guidance and associated reference documents provided for the control in NIST SP 800-53 to assist in determining if the control is not applicable.
  - Typically controls which do not apply to a system are tailored out of the control baseline by the organization in RMF Step 2, Select.

The SO is responsible for producing a Plan of Action and Milestones (POA&M) for all planned controls deemed less than effective.

13.4. Component 4 of 8: Supplemental C-SCRM Guidance

Supplemental C-SCRM guidance provides non-prescriptive, additional information for control implementation.

13.5. Component 5 of 8: Control Baseline Allocation

Baseline allocation is the assignment of minimum-security requirements for Federal systems and a risk-based process for selecting the controls necessary to satisfy the minimum requirements.

OMB Circular A-130, Section 10, Definitions, describes a Federal information system as: A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information. Section 10 also clarified that Federal information systems are those used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

13.6. Component 6 of 8: Control Parameter

The Control Parameter (also called organization-defined parameter) provides a degree of flexibility by allowing organizations to define values for certain parameters associated with the controls.

- Control Parameters are predefined assignment and selection statements embedded within the controls and control enhancements separated by brackets. (e.g., *[annually or whenever there is a change in the system's threat environment]*)
- Assignment and selection statements provide organizations with the capability to tailor controls and control enhancements based on: (i) Security requirements to support organizational missions/business functions and operational needs; (ii) Risk assessments and organizational risk tolerance; and (iii) Security requirements originating in Federal laws, Executive Orders, directives, policies, regulations, standards, or guidelines.
- Once specified, the organization-defined values for assignment and selection statements become part of the security control, and the control implementation is assessed against the completed control statement.

Implementation statements must include how the system meets the control parameter requirements. **Do not change the language of the GSA ODP in the Control Section.**

Control Parameters which state system-specific parameter require an organization to specify in the implementation statement the organization system-specific parameter.

13.7. Component 7 of 8: Control Section

The Control Section provides a concise control implementation statement of the specific security, privacy, or C-SCRM capabilities which are implemented, as well as the following:

- Contains the security, privacy, and/or C-SCRM requirements for the system and the controls selected by the organization to satisfy the minimum baseline requirements.
- Describes the activities or actions, automated or non-automated, needed to be carried out by systems, organizations, and individuals to implement a control.
    - SOs are expected to be compliant with and respond to all parts of a control section (e.g., Part a, b, c, etc.).
- May contain control parameters that must be implemented by the system and included in the control implementation statements.

The Control Sections have been designed to facilitate compliance with applicable laws, Executive Orders, directives, policies, regulations, and standards.

13.8. Component 8 of 8: Control Implementation Statements

The Control Implementation Statement describes the implementation or intended implementation of each control in the context of the system with a sufficient level of detail to correctly implement the control and to subsequently assess the effectiveness of the control. It also contains the following attributes:

- Must describe how the control is being implemented or planned to be implemented on each applicable platform (e.g., Windows, Unix/Linux, Database, Web, etc.).
- The implementation of the control is assessed against the completed control statement.
- Contributes to the overall organization-defined capability.
- Can address a variety of areas that can include technical means, physical means, procedural means, or any combination thereof.

By properly documenting control implementations, organizations can obtain greater visibility into and a better understanding of: (i) The intended or actual implementation of the controls implemented within the system; (ii) The relationships (i.e., dependencies) among controls; and (iii) The potential severity of control weaknesses or deficiencies.

13.9. Control Implementation Statement (Requirements, Explanations, and Examples)

13.9.1. Responsibilities for Common Control Requirements

To inherit a particular control, the following conditions must be true:

- The control is implemented and managed outside the authorization boundary of the inheriting system.
- The common control provider has designated the control as inheritable.
- The common control provider has an Authorization to Operate (ATO) or equivalent evidence that the control is in fact in place.

The common control provider is responsible for:

- Documenting common controls in a system security, privacy, and/or C-SCRM Plan
- Ensuring that common controls are developed, implemented, and assessed for effectiveness by qualified assessors with a level of independence required by the organization.
- Receiving authorization for the common controls from the designated authorizing official (if applicable)

- Monitoring common control effectiveness on an ongoing basis

> There is no requirement to provide implementation details for inherited common controls. Rather, those

13.9.2. Common Control Implementation Statement Explanation

Common controls are controls which can support multiple systems efficiently and effectively as a common capability. They are a single implementation leveraged and used uniformly across the organization and by inheriting systems.

The organization may choose, for example, to implement security control CA-1 (Policy and Procedures) by establishing policy and procedures for the effective implementation of selected controls and control enhancements in the Assessment, Authorization, and Monitoring (CA) family that must be adhered to by all organizational and inheriting systems.

For each control section (i.e., Part a, Part b, Part c, etc.), provide a thorough description of how the control is implemented. Include references to any relevant artifacts that support control implementation.

- For Common controls, only complete the orange row(s)

The following example shows one way a common control implementation of a control and minimum assurance requirements can be documented in the C-SCRM Plan. It is not a mandatory format. Organizations may develop their own unique method to capture the information, consistent with the requirements in NIST SP 800-161 Rev. 1 and NIST SP 800-53 Rev. 5.

SECURITY ASSESSMENT AND AUTHORIZATION (CA)				
CA 1 Security Assessment and Authorization Policy and Procedures				
IMPLEMENTATION STATUS	CONTROL ORIGINATION			
Implemented	*Common Control*			
NIST SP 800 53 CONTROL BASELINE ALLOCATION:	Privacy	Low	Moderate	High
NIST SP 800 161 CONTROL BASELINE ALLOCATION:	C SCRM	Level 1	Level 2	Level 3
Supplemental C-SCRM Guidance:	Integrate the development and implementation of assessment and authorization policies and procedures for supply chain cybersecurity into the control assessment and authorization policy, and related C-SCRM Strategy/Implementation Plan(s), policies, and system-level plans. To address cybersecurity risk in the supply chain, enterprises should develop a C-SCRM policy (or, if required, integrate into existing policies) to direct C-SCRM activities for control assessment and authorization. The C-SCRM policy should define C-SCRM roles and responsibilities within the enterprise for conducting control assessment and authorization, any dependencies			

SECURITY ASSESSMENT AND AUTHORIZATION (CA)	
CA 1 Security Assessment and Authorization Policy and Procedures	
	among those roles, and the interaction among the roles. Enterprise-wide security and privacy risk should be assessed on an ongoing basis and include supply chain risk assessment results.
Part a	a. Develop, document, and disseminate to *[personnel with IT security responsibilities as defined in Security Assessment and Authorization policy]*: 1. A security assessment and authorization policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security assessment and authorization policy and associated security assessment and authorization controls;
System-Specific	
Common or Hybrid	This control is an inherited common control and is implemented and managed outside of the ACME system authorization boundary by the Agency X. Agency X's common control provider is responsible for fully implementing Part a of this control. Refer to Agency X's common control provider's security authorization package for implementation details regarding this common control or Agency X's Information Security Program Plan, Revision 2, dated 14 March 2022, Section 3.4.1, Security Assessment and Authorization Policies and Procedures (CA-1).

Figure 13 - Common Control Example

13.9.3. Responsibilities for System-Specific Control Requirements

The SO is responsible for:

- Documenting system-specific controls in the C-SCRM Plan
- Ensuring system-specific controls are developed, implemented, and assessed for effectiveness by qualified assessors with a level of independence required by the organization
- Documenting planned system-specific control in a security assessment report
- Producing a Plan of Action and Milestones (POA&M) for all system-specific controls deemed less than effective (i.e., having weaknesses or deficiencies in the controls)
- Receiving authorization for the system-specific controls from the designated authorizing official (if applicable)
- Monitoring system-specific control effectiveness on an ongoing basis

13.9.4. System-Specific Control Explanation

System-Specific controls are security controls which provide a security capability for a particular system and are the primary responsibility of SOs and their respective authorizing officials (if applicable). The implementation is unique to the specific system.

An example of a control that is typically implemented as a system-specific control is AC-7 (Unsuccessful Logon Attempts) where the system enforces limits on consecutive invalid logon attempts and automatically locks the account when the maximum number of unsuccessful attempts is exceeded during the authentication process.

> For each control section (i.e., Part a, Part b, Part c, etc.), provide a thorough description of how the control is implemented. Include references to any relevant artifacts that support control implementation.
>
> - For System-Specific controls, only complete the blue row(s)

The following example shows one way a system-specific control implementation of the control and minimum assurance requirements can be documented in the C-SCRM Plan. It is not a mandatory format. Organizations may develop their own unique method to capture the information, consistent with the requirements in NIST SP 800-161 and NIST SP 800-53.

ACCESS CONTROL (AC)

AC 7 Unsuccessful Logon Attempts

IMPLEMENTATION STATUS	CONTROL ORIGINATION			
Implemented	Choose an item.			
NIST SP 800 53 CONTROL BASELINE ALLOCATION:	Privacy	Low	Moderate	High
NIST SP 800 161 CONTROL BASELINE ALLOCATION:	C SCRM	Level 1	Level 2	Level 3

Supplemental C-SCRM Guidance:	The need to limit unsuccessful logon attempts and take subsequent action when the maximum number of attempts is exceeded applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are usually temporary and automatically release after a predetermined, organization-defined time.
Part a	a. Enforces a limit of *[not more than ten (10) failed access attempts]* consecutive invalid logon attempts by a user during a *[30-minute time period]*; and
System-Specific	The "ACME System Access Control Policy" v.10, dated 05 May 2022, Section 9, Unsuccessful Logon Attempts, states that the ACME account lockout threshold policy prevents brute-force password attacks on the system while allowing for honest errors made during a normal user logon. ACME system administrators must configure operating system and application-level account lockout threshold group policy settings in active directory to a value of three (3). This will cause an account to be locked after three (3) consecutive invalid logon attempts within the specified time period as listed below. The "ACME System Access Control Policy" v.10, dated 05 May 2022, Section 10, Logon Delay Algorithm, states that the ACME logon delay algorithm policy prevents brute-force password attacks on the system while allowing for honest errors made during a normal user logon. ACME system administrators must configure operating system and application-level account logon delay algorithm group policy settings in active directory

ACCESS CONTROL (AC)	
AC 7 Unsuccessful Logon Attempts	
	to a value of 15 minutes. This enforces a limit of three (3) consecutive invalid logon attempts by a user during a 15-minute time period.
Common or Hybrid	
Part b	b. Automatically *[locks the account node for [30 minutes]]* when the maximum number of unsuccessful attempts is exceeded.
System-Specific	The "ACME System Access Control Policy" v.10, dated 05 May 2022, Section 11, Account Lockout Duration, states that the ACME account lockout duration policy prevents denial of service attacks on the system while balancing against the cost of ACME Help Desk support for password resets. ACME system administrators must configure operating system and application-level account lockout duration group policy settings in active directory to a value of 15 minutes. This will cause an account to be temporarily and automatically locked for 15 minutes before being reset or until a system administrator manually unlocks the account after three (3) unsuccessful logon attempts
Common or Hybrid	

Figure 14 - System-Specific Control Example

13.9.5. Responsibilities for Hybrid Control Requirements

The common control provider is responsible for the development, implementation, assessment, and monitoring of the common portion of hybrid controls. Additional common control provider responsibilities include:

- Documenting the common portion of hybrid controls in the C-SCRM Plan
- Ensuring the common portion of hybrid controls are developed, implemented, and assessed for effectiveness by qualified assessors with a level of independence required by the organization.
- Receiving authorization for the common portion of hybrid controls from the designated authorizing official (if applicable)
- Monitoring common portion of hybrid control effectiveness on an ongoing basis

For hybrid controls, the organization specifies in the system-level C-SCRM plans, the parts of the control that are provided by the common control provider and the parts of the control that are implemented at the system level.

The SO is responsible for the development, implementation, assessment, and monitoring of the system-specific portion of hybrid controls. Additional SO responsibilities include:

- Documenting the system-specific portion of hybrid controls in the C-SCRM Plan

- Ensuring the system-specific portion of hybrid controls are developed, implemented, and assessed for effectiveness by qualified assessors with a level of independence required by the organization.
- Receiving authorization for the system-specific portion of hybrid controls from the designated authorizing official (if applicable)
- Monitoring system-specific portions of hybrid control effectiveness on an ongoing basis

For hybrid controls, the SO specifies in the C-SCRM Plan, the parts of the control that the SO is responsible for and the parts of the control that are implemented by the common control provider.

13.9.6. Hybrid Control Implementation Statement Explanation

Hybrid controls are controls where one part of the control is deemed to be common and another part of the control is deemed to be system-specific. The implementation is split between two or more elements or organizations.

The organization may choose, for example, to implement security control CP-2 (Contingency Plan) by providing a template for a generalized contingency plan for all organizational systems with individual SOs tailoring the plan, where appropriate, for system-specific uses.

For each control section (i.e., Part a, Part b, Part c, etc.), provide a thorough description of how the control is implemented. Include references to any relevant artifacts that support control implementation.

- For Hybrid controls, complete both the blue and orange rows.

The following example shows one way a hybrid control implementation of the control and minimum assurance requirements can be documented in security and privacy plans. It is not a mandatory format. Organizations may develop their own unique method to capture the information, consistent with the requirements in NIST SP 800-161 and NIST SP 800-53.

INCIDENT RESPONSE (IR)

IR 6 Incident Reporting

IMPLEMENTATION STATUS	CONTROL ORIGINATION
Implemented	*Hybrid Control*

NIST SP 800 53 CONTROL BASELINE ALLOCATION:	Privacy	Low	Moderate	High
NIST SP 800 161 CONTROL BASELINE ALLOCATION:	C SCRM	Level 1	Level 2	Level 3

Supplemental C-SCRM Guidance:	Communications of security incident information from the enterprise to suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers and vice versa require protection. The enterprise should ensure that information is reviewed and approved for sending based on its agreements with suppliers and any relevant interagency bodies. Any escalation of or exception from this reporting should be clearly defined in the agreement. The enterprise should ensure that incident reporting data is adequately protected for transmission and received by approved individuals only. Enterprises should require their prime contractors to implement this control and flow down this requirement to relevant sub-tier contractors.
Part a	a. Require personnel to report suspected incidents to the organizational incident response capability within *[US-CERT Incident Reporting Timelines]*; and
System-Specific	
Common or Hybrid	The common portion of this hybrid control is inherited, implemented, and managed outside the ACME system authorization boundary for Agency X. Agency X's common control provider is responsible for fully implementing Part a of this control. Refer to Agency X's common control provider's security authorization package for implementation details regarding this common control or Section 3.8.6, Incident Reporting (IR-6), of Agency X's Incident Response (IR) Procedures, Revision 2, dated 14 March 2022.
Part b	b. Report incident information to *[Report incidents to business partners, outside agencies, including law enforcement, regulatory bodies and information sharing organizations such as InfraGard and the industry Information Sharing and Analysis Centers (ISACs)]*.
System-Specific	The ACME system's SO reports identified security incident information within the required one hour time frame to Agency X by completing the incident reporting form identified in Appendix B of Agency X's Incident Response (IR) Procedures, Revision 2, dated 14 March 2022, and submitting the report via email to the Agency X Service Desk at servicedesk@AgencyX.gov, carbon copying the Agency X Incident Response Team at irteam@AgencyX.gov, Office of the Chief Information Security Officer (OCISO), and Contracting Officer.
Common or Hybrid	

Figure 15 - Hybrid Control Example

13.9.7. Dash 1 Policy and Procedures Control Requirements

A Dash 1 control is the first control in each family (e.g., AC-1) and addresses the establishment of policy and procedures for the effective implementation of the controls and control enhancements within a control family.

- NIST 800-53, Dash 1 (policy and procedure controls) include requirements to ensure the organization is developing and documenting policies; and implementing remediation actions for violations of policy. This process applies to policy items that do not tie to a specific NIST SP 800-53 Rev. 5 control as remediation actions tied to control failures are noted in a POA&M.
- NIST SP 800-53 Rev. 5 states in the Discussion section of the Dash 1 controls: "Simply restating controls does not constitute an organizational policy or procedure."
- It is recommended that organization policy and organization procedures be documented in separate documents.

Comprehensive policy and procedures help provide security, privacy, and supply chain assurance.

Security, privacy, and C-SCRM program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary.

The Dash 1 control generates requirements for specific policies and procedures which are needed for the effective implementation of the other security, privacy, or C-SCRM controls in the family.

All Dash 1 control implementation statements generally should be identical excluding the name of the policy and procedures.

When referencing policies and procedures, be sure to cite the document's proper name, version number, and revision date.

The following example shows one way to accurately document Dash 1 control implementation of the control and minimum assurance requirements in the C-SCRM Plan. It is not a mandatory format. Organizations may develop their own unique method to capture the information, consistent with the requirements in NIST SP 800-161 Rev. 1 and NIST SP 800-53 Rev. 5.

CONFIGURATION MANAGEMENT (CM)

CM 1 Configuration Management Policy and Procedures

IMPLEMENTATION STATUS	CONTROL ORIGINATION
Implemented	*System Specific Control*

NIST SP 800 53 CONTROL BASELINE ALLOCATION:	Privacy	Low	Moderate	High
NIST SP 800 161 CONTROL BASELINE ALLOCATION:	C SCRM	Level 1	Level 2	Level 3

Supplemental C-SCRM Guidance:	Configuration management impacts nearly every aspect of the supply chain. Configuration Management is critical for enterprise's ability to establish provenance of components, including tracking and tracing them through the SDLC and the supply chain. A properly defined and implemented configuration management capability provides greater assurance throughout the SDLC and the supply chain that components are authentic and have not been inappropriately modified. When defining a configuration management policy and procedures, enterprises should address the full SDLC, including procedures for introducing and removing components to and from the enterprise's system boundary. A configuration management policy should incorporate configuration items, data retention for configuration items and corresponding metadata, and tracking of the configuration item and its metadata. The enterprise should coordinate with suppliers, developers, system integrators, external system service providers, and other ICT/OT-related service providers regarding the configuration management policy.
Part a	a. Develop, document, and disseminate to *[personnel with configuration management responsibilities]*: 1. A configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the configuration management policy and associated configuration management controls; and
System-Specific	The ACME compliance team has developed and documented configuration management policy and procedures that, per the "ACME Risk Management Policy" v.17, dated 23 April 2022, are disseminated annually via the internal ACME compliance team web portal to all personnel in roles that are directly responsible for the cybersecurity, system administration, configuration, management, oversight, and successful day-to-day operations of ACME hardware, software, and applicable documentation. The "ACME Configuration Management Policy" v.3, dated 05 May 2022, addresses purpose in Section 1, scope in Section 2, roles and responsibilities in Section 3, management commitment in Section 4, coordination among organization entities in Section 5, and compliance in Section 6. The "ACME Configuration Management Procedures" v.12, dated 05 May 2022, facilitate the implementation of the "ACME Configuration Management Policy "and associated National Institute of Standards and Technology (NIST) configuration management controls to manage and control the moderate categorized system baselines of all ACME technology stacks within the authorization boundary.
Common or Hybrid	.
Part b	b. Reviews and updates the current: 1. Configuration management policy *[Annually]*; and 2. Configuration management procedures *[Annually]*.

	" " " "
Common or Hybrid	

Figure 16 - Dash-1 Control Example

13.9.8. Not Applicable Control Requirements

Review each control and determine if the control does or does not apply to the system or specific components within the system based on the system's operational conditions. If the control does not apply to the system, mark the control as "Not Applicable" in the control implementation status section and explain the rationale justifying why the control does not apply. If the control does not apply to specific components in the system (e.g., remote sensors), identify the component to which the control does not apply.

Controls that are Not Applicable:

- Must have a justification of why the requirement does not apply included in the control implementation statement.
- The system owner should read the supplemental guidance and associated reference documents provided for the control in NIST SP 800-53 to assist in determining if the control is truly not applicable.
- In cases where the system is unable to deem a control as applicable or not applicable, the system owner should contact the system security officer or privacy officer for clarification.

It is very rare to have a security or privacy control with an implementation status of Not Applicable. For example, if an information system does not have wireless access (AC-18), the security control should not be marked as "Not Applicable." The organization should mark the control as In-Place and explain; for example, their implementation of a wireless access restriction policy as well as a WIPS for detection of rogue Wi-Fi devices within the authorization boundary.

The following example shows one way a Not Applicable control implementation of the control and minimum assurance requirements can be documented in the C-SCRM Plan. It is not a mandatory format. Organizations may develop their own unique method to capture the information, consistent with the requirements in NIST SP 800-161 and NIST SP 800-53.

SYSTEM AND COMMUNICATIONS PROTECTION (SC)				
SC 19: Voice Over Internet Protocol				
IMPLEMENTATION STATUS	**CONTROL ORIGINATION**			
Not Applicable	*System Specific Control*			
NIST SP 800 53 CONTROL BASELINE ALLOCATION:	Privacy	Low	Moderate	High
NIST SP 800 161 CONTROL BASELINE ALLOCATION:	C SCRM	Level 1	Level 2	Level 3
Supplemental C-SCRM Guidance:	None			
Part a	a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the system if used maliciously; and			
System-Specific	This control is Not Applicable. Currently the ACME system has not implemented Voice over Internet Protocol (VoIP). All VoIP traffic is blocked at the Cisco 4331 Integrated Services Router (ISR) by access control lists (ACLs). Therefore, this control does not apply to the system environment.			
Common or Hybrid				
Part b	b. Authorizes, monitors, and controls the use of VoIP within the system.			
System-Specific	This control is Not Applicable. Currently the ACME system has not implemented VoIP. All VoIP traffic is blocked at the Cisco 4331 ISR by ACLs. Therefore, this control does not apply to the system environment.			
Common or Hybrid				

Figure 17 - Not Applicable Control Example

13.9.9. Planned Control Requirements

Documentation of planned control implementation allows for traceability of decisions prior to and after the deployment of the system.

- Controls selected as planned must document a scheduled plan for achieving full implementation of the control.
- Planned control implementations must be monitored to ensure proper and scheduled deployment.
- Planned control implementations must be documented in the POA&M to be reviewed by the authorizing official (if applicable) to ensure there is agreement with the remediation actions planned to correct the identified deficiencies, thereby permitting informed judgments and investments that respond to identified risks in an acceptable manner.

- It is recommended that planned control implementation statements include supporting countermeasures and/or compensating controls that are proven to directly reduce the risk of the control deficiency being compromised.
- Once a planned control is implemented, the control status and control implementation statement in the C-SCRM Plan must be updated to reflect the current control deployment.

It is unlikely that all controls can be fully implemented by the time the accreditation is achieved. To permit the system to operate at an acceptable level of risk based on minimum NIST security requirements being met, the SO should take action to implement Planned controls specified in the C-SCRM Plan as rapidly as resources permit.

The organization may choose, for example, to plan to implement the Information Input Validation control (SI-10) by identifying all inputs from potentially untrusted users, to eliminate the inputs or make it impossible for untrusted users to provide information to them.

The following example shows one way a Planned control implementation of the control and minimum assurance requirements can be documented in the C-SCRM Plan. It is not a mandatory format. Organizations may develop their own unique method to capture the information, consistent with the requirements in NIST SP 800-53 Rev. 5.

SYSTEM AND INFORMATION INTEGRITY (SI)				
SI 10: Information Input Validation				
IMPLEMENTATION STATUS	**CONTROL ORIGINATION**			
Planned	*System Specific Control*			
NIST SP 800 53 CONTROL BASELINE ALLOCATION:	Privacy	Low	Moderate	High
NIST SP 800 161 CONTROL BASELINE ALLOCATION:	C SCRM	Level 1	Level 2	Level 3
Supplemental C-SCRM Guidance:	Checking the valid syntax and semantics of system inputs—including character set, length, numerical range, and acceptable values—verifies that inputs match specified definitions for format and content.			
Part a	a. The system checks the validity of *[Character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content as it relates to: (1) Username and password combinations. (2) Attributes used to validate a password reset request (e.g., security questions). (3) Personally identifiable information (excluding unique username identifiers provided as a normal part of a transactional record). (4) Biometric data or personal characteristics used to authenticate identity. (5) Sensitive financial records (e.g., account numbers, access codes). (6) Content related to internal security functions: private encryption keys, whitelist or blacklist rules, object permission attributes and settings]*.			
System-Specific	This control implementation is planned. The ACME system developers plan to identify and test all input strings supplied by a user or application that an attacker can manipulate. When developers find any fields that can receive improperly formed data, those fields will be logged and inventoried to be remediated. Input validation			

SYSTEM AND INFORMATION INTEGRITY (SI)	
SI 10: Information Input Validation	
	will be applied to ensure only properly formed data is entering the workflow of a system at both syntactical and semantic levels using whitelisting filters and input/output sanitization. The ACME system developers plan to remediate this deficient control by 31 December 2022. See ACME's Plan of Action and Milestones (POA&M) for more details regarding the planned implementation of this control. To provide defense-in-depth for this control and to prevent attack payloads, ACME system developers will encrypt view state if any of the data is application-sensitive, upgrade to the latest version of ASP.NET as soon as practical and move truly sensitive view state data to the session variable.
Common or Hybrid	.

Figure 18 - Planned Control Example

13.9.10. Technology Stack Requirements

Understanding the technology stack (the hardware and software products that the infrastructure is built on), is important for the proper documentation of implementation statements for all platforms, whether speaking to controls that apply to a major application or to a general support system.

- Each technology stack must be protected and secured using the control catalog in NIST SP 800-161 Rev. 1 and NIST SP 800-53 Rev. 5.
- Implementation statements must speak to how the controls are implemented on each technology stack or platform (e.g., network devices, databases, operating systems, web applications, etc.).
- All technology stacks must be documented in the system component inventory. If a technology stack is spoken to in an implementation statement and not documented in the system component inventory or vice versa, these inconsistencies will be red flagged by the control assessor and cause the control implementation status to be marked as "Planned" or "Partially Implemented."

Cybersecurity must be an integrated set of services to protect all technology stacks. Building cybersecurity into technology stacks is a multi-layered approach sometimes referred to as a "defense-in-depth" approach, designed to defend a system against attacks using several different methods; if one defensive measure fails, then the others will stop the threat.

SOs must write to each technology stack, for clarity, when communicating how a system is securely architected.

An example of a security control that typically requires multiple implementation statements to cover all technology stacks deployed in the authorization boundary is RA-5 (Vulnerability Monitoring and Scanning). The SO determines the required vulnerability scanning for all system

components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked.

This following example shows one way each technology stack control implementation is documented in the C-SCRM Plan. It is not a mandatory format. Organizations may develop their own unique method to capture the information, consistent with the requirements in NIST SP 800-161 Rev. 1 and NIST SP 800-53 Rev. 5.

RISK ASSESSMENT (RA)				
RA 5: Vulnerability Monitoring and Scanning				
IMPLEMENTATION STATUS	CONTROL ORIGINATION			
Implemented	*System Specific Control*			
NIST SP 800 53 CONTROL BASELINE ALLOCATION:	Privacy	Low	Moderate	High
NIST SP 800 161 CONTROL BASELINE ALLOCATION:	C SCRM	Level 1	Level 2	Level 3
Supplemental C-SCRM Guidance:	Checking the valid syntax and semantics of system inputs—including character set, length, numerical range, and acceptable values—verifies that inputs match specified definitions for format and content.			
Part a	a. Scans for vulnerabilities in the system and hosted applications *[weekly for operating systems (OS)-including databases, monthly unauthenticated web application scans, annual authenticated web application scans (quarterly for systems in Ongoing Authorization using Single Sign On as a front end to the application)]* and when new vulnerabilities potentially affecting the system/applications are identified and reported.			
System-Specific	**Network:** As per the "ACME Vulnerability Scanning Policy" v12.1, dated 18 April 2022, Section 8, Vulnerability Scanning Frequency, the ACME compliance team monitors, and scans for vulnerabilities on a weekly basis on all network devices with Titania Nipper version 2.13.0. The ACME compliance team conducts rescans as needed when new vulnerabilities potentially affecting the system are identified and reported by the Cybersecurity and Infrastructure Security Agency (CISA). **Operating Systems:** As per the "ACME Vulnerability Scanning Policy" v12.1, dated 18 April 2022, Section 8, Vulnerability Scanning Frequency, the ACME compliance team monitors and scans weekly for vulnerabilities on all operating systems with Tenable Nessus 8.0.0. The ACME compliance team conducts rescans as needed when new vulnerabilities potentially affecting the system are identified and reported by CISA. **Database:** As per the "ACME Vulnerability Scanning Policy" v12.1, dated 18 April 2022, Section 8, Vulnerability Scanning Frequency, the ACME compliance team monitors, and scans weekly for vulnerabilities on all databases with Trustwave AppDetectivePRO 8.7. The ACME compliance team conducts rescans as needed when new vulnerabilities potentially affecting the system are identified and reported by CISA. **Web Applications:**			

RISK ASSESSMENT (RA)
RA 5: Vulnerability Monitoring and Scanning

Figure 19 - Technology Stack Example

13.9.11. Comparison of Well-Written vs. Poorly Written Control Implementation Statement Examples

Below is a comparison of a Well-Written vs. Poorly Written Control Implementation Statement.

CONFIGURATION MANAGEMENT (CM)					
CM 6(1): Configuration Settings | Automated Management, Application, and Verification					
IMPLEMENTATION STATUS		**CONTROL ORIGINATION**			
Implemented		*System Specific Control*			
NIST SP 800 53 CONTROL BASELINE ALLOCATION:		Privacy	Low	Moderate	High
NIST SP 800 161 CONTROL BASELINE ALLOCATION:		C SCRM	Level 1	Level 2	Level 3
Supplemental C-SCRM Guidance:	The enterprise should, when feasible, employ automated mechanisms to manage, apply, and verify configuration settings.				
Part a	a. The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for *[all operating systems]*.				
System-Specific	The "ACME Configuration Management Procedures" v.12, dated 05 May 2022, Section 15.1, Automated Configuration Management states: ACME's adoption of various platform specific software configuration management tools helps reduce the security risk that can result from configuration changes. ACME centrally manages, applies, and verifies configuration settings with the use of the following tools: **Windows:** For Windows 10 and Windows Server 2019, ACME has deployed McAfee ePolicy Orchestrator 5.10.x the most advanced, extensible, and scalable centralized security management software in the industry. **Unix/Linux/MAC:** For Red Hat Enterprise Linux (RHEL) 6.6 and MAC OS 10.14, ACME has deployed BeyondTrust Likewise v6.5 to enable configuration management in ACME's cross-platform environments. **Database:**				

CONFIGURATION MANAGEMENT (CM)	
CM 6(1): Configuration Settings | Automated Management, Application, and Verification	
	- -

Figure 20 - Well-Written Implementation Statement Example

CONFIGURATION MANAGEMENT (CM)				
CM 6(1): Configuration Settings | Automated Management, Application, and Verification				
IMPLEMENTATION STATUS	**CONTROL ORIGINATION**			
Implemented	*System Specific Control*			
NIST SP 800 53 CONTROL BASELINE ALLOCATION:	Privacy	Low	Moderate	High
NIST SP 800 161 CONTROL BASELINE ALLOCATION:	C SCRM	Level 1	Level 2	Level 3
Supplemental C-SCRM Guidance:	The enterprise should, when feasible, employ automated mechanisms to manage, apply, and verify configuration settings.			
Part a	a. The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings for *[all operating systems]*.			
System-Specific	ACME system employs automated mechanisms to centrally manage, apply, and verify configuration settings for all operating systems.			
Common or Hybrid	.			

Figure 21 - Poorly Written Implementation Statement Example

13.10. Security Control Implementation Review Checklist

Risk can be more effectively understood and managed if the risk is clearly articulated. The key to writing a good implementation statement is having a foundational understanding of the security controls and their interrelationships. Understanding key security-related terms and their definitions, as well as the systems mission and business objectives, will result in more precise and

impactful implementation statement articulation. Summarizing control implementations in a statement is not a science and there is no specific formula to get it right; however, the guidance provided in review checklist below can help to better articulate control implementations.

13.10.1. Resources and Training

- ❑ Allocate sufficient time and effort for writing.
- ❑ Ensure the individuals who are writing the documentation have the required expertise and knowledge of NIST controls.
- ❑ Allocate enough resources - Often one writer is not enough, and additional resources and subject matter experts may be required to complete the C-SCRM Plan.
- ❑ Ensure the writers have technical knowledge of the system or can obtain the information from the SO.
- ❑ When writing, present the who, what, when, where, why, and how of the system.
- ❑ Read control implementation guidance in NIST SP 800-37 Rev. 2, Appendix F, System and Common Control Authorizations; Authorization Package section, for the proper status of security controls as implemented or planned.
- ❑ Read control origination guidance in NIST SP 800-37 Rev. 2, Chapter Three, The Process; Section 3.3, Select Tasks; Control Allocation Task S-3, for the proper allocation of security controls as system-specific, hybrid, or common controls.

13.10.2. Grammar and Writing Conventions

- ❑ Use the correct and most recent C-SCRM Plan template and do not modify or remove sections.
- ❑ Use consistent terminology throughout the C-SCRM Plan.
- ❑ Run a spelling and grammar check.
- ❑ Spell out full expansions for the first use of all acronyms.
- ❑ When referencing documentation, include the document name, version, and revision date. When referencing details in a document, add the section number.
- ❑ When referencing hardware or software, include the vendor's name, application/device name, and model/version.
- ❑ Strongly and clearly articulate security architecture and implementations.

- ❑ Be clear, concise, consistent, and thorough.
- ❑ Be direct and to the point - Avoid run-on sentences and use of the passive voice; use present tense and active voice.
- ❑ After all descriptions are written, read through the control implementation descriptions to check for:
    - ❑ Errors not discovered by grammar/spell-check.
    - ❑ Checkboxes that have not been appropriately marked.
    - ❑ Every control part (Part a, Part b, Part c, etc.) and subpart should be clearly notated and contain a focused discussion on the specific control requirement.

13.10.3. Control Implementation Statements

- ❑ Ensure compliance with Federal policy and procedures
- ❑ When filling out the C-SCRM Plan, be sure to answer 100% of the controls and each control part individually if control parts are used in the control.
- ❑ Be sure to speak to how the control parameter is being met.
- ❑ Do not parrot back the control requirements. Document the control implementation, as appropriate, in the C-SCRM Plan, providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs). Supporting materials such as procedures, reports, logs, and records showing evidence of control implementation should be identified as well.
- ❑ Do not use boilerplate text which is repetitive throughout the document.
- ❑ Address all applicable platforms (Windows, Unix/Linux, Database, Web, etc.) and answer the "who, what, when, where, and how" the control is compliant with agency requirements.
- ❑ Ensure the statements stand on their own so the reader is not required to read additional documentation.

APPENDIX A - ACRONYMS

When creating a large document, such as a C-SCRM Plan, it could contain many abbreviations. If so, it is a requirement to add a list of acronyms and abbreviations to help the reader. When introducing a new abbreviation, define it first in Appendix A, Acronyms. Typically, this list will:

- Appear in the end of the document
- List all abbreviations, acronyms, and initialisms alphabetically

- Define each abbreviation alongside its shortened form

List the acronyms of the abbreviated words used in the C-SCRM Plan in the Appendix A table. The table is available in the C-SCRM Plan Template.

APPENDIX B - RELATED LAWS AND REGULATIONS

In the C-SCRM Plan Template, this section contains boilerplate text that provides a reference to C-SCRM standard laws, regulations, and/or polices. Update the boilerplate text, where appropriate; and add any vendor specific plans, polices, processes, and procedures. List any laws, regulations, or policies that establish specific requirements for confidentiality, integrity, or availability of data stored, processed, or transmitted by the system. The Computer Security Act of 1987, OMB Circular A-130, and general agency security requirements need not be listed since they mandate security for all systems. Each organization should decide on the level of laws, regulations, and policies to include in the C-SCRM Plan. Examples might include the Privacy Act or a specific statute or regulation concerning the information processed (e.g., tax or census information). If the system processes records subject to the Privacy Act, include the number and title of the Privacy Act system(s) of records and whether the system(s) are used for computer matching activities.

APPENDIX C - C-SCRM ACTIVITIES AND LIFE CYCLES

The C-SCRM Plan should cover the full System Development Life Cycle (SDLC) of systems and programs, including research and development, design, manufacturing, acquisition, delivery, integration, operations, and disposal/retirement. The C-SCRM plan activities should be integrated into the enterprise's system and software life cycle processes to ensure that C-SCRM activities are integrated into those processes. Similar controls in the C-SCRM Plan can be applied in more than one life cycle process. The figure below shows how the C-SCRM plan activities can be integrated into various example life cycles.

Contextualize the components from Section 6.2, Network Diagrams and Section 6.3, System Component Inventory of the C-SCRM Plan against the system's SDLC to ensure activities are mapped and tracked. This ensures full coverage of C-SCRM activities since these activities may require repeating and reintegrating (using spiral or agile techniques) throughout the life cycle. C-SCRM plan activities are required from concept, all the way through development, production, utilization, support, and retirement steps.

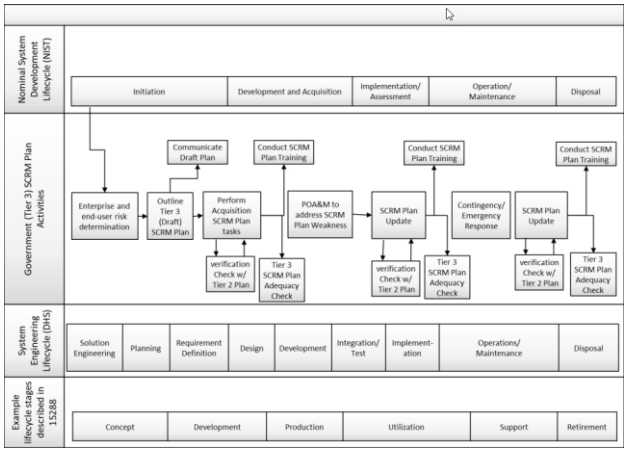

Figure 22 - SDLC Diagram Example

APPENDIX D - ATTACHMENTS

Attach any relevant artifacts that can be included to support the C-SCRM Plan.

To insert an object, click **Object** (or the **Object icon** in the Text ribbon) on the **Insert** tab:

1. In the Object dialog box, select the **Create from File** tab, and then click the **Browse…** button to find the file to insert.
2. To make the inserted file to appear as a clickable icon, rather than the first page of the file, select **Display as icon** check box. If this check box is selected, a different icon can be chosen by clicking the **Change Icon…** button.

Below is an ancillary document that is included to support the C-SCRM Plan.

Attachment 1 System Component Inventory

Figure 23 - Attachment Example

Recommended attachments include, but are not limited to, the following:

1. Plan of Action and Milestones (POA&M)
2. Contingency Plan
3. Incident Response Plan
4. Continuous Monitoring Strategy
5. System and services acquisition policy
6. System and services acquisition procedures
7. Supply chain risk management policy
8. Supply chain risk management procedures

APPENDIX E - C-SCRM CONTROL IMPLEMENATION SUMMARY (CIS)

For each control, select the implementation status via the drop-down menu in the table. If the control implementation status is "Planned," select an estimated completion date from the pop-up calendar in the adjoining column.

Control Identifier	Control Name	Implementation Status	Estimated Completion Date
AC-2	Account Management	Implemented	
AT-3	Role-Based Training	Implemented	
AU-2	Event Logging	Planned	4/26/2023
AU-6	Audit Record Review, Analysis, and Reporting	Implemented	
CA-5	Plan of Action and Milestones	Implemented	

Figure 24 - Control Implementation Summary Example