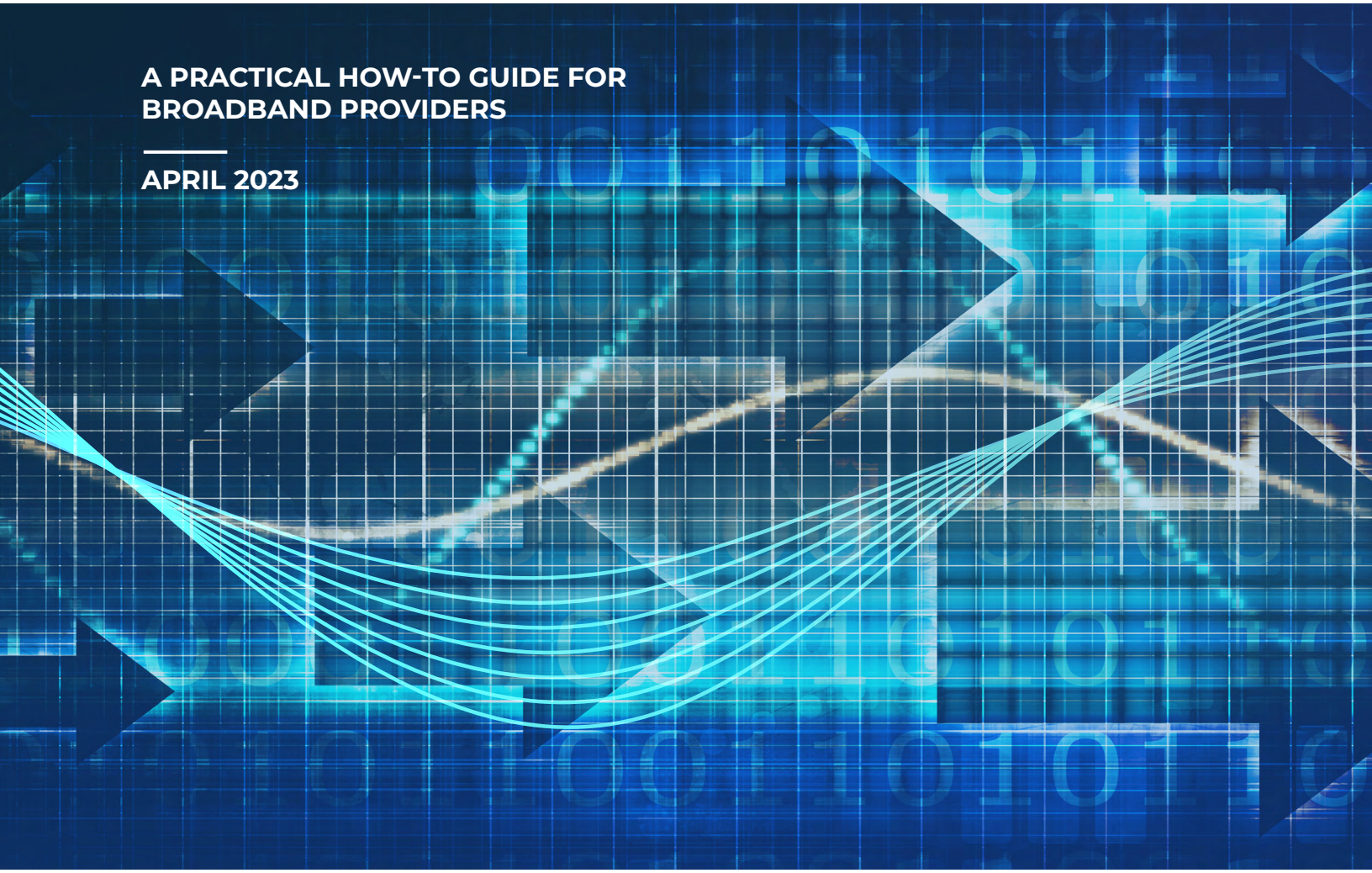
BROADBAND EQUITY, ACCESS, AND DEPLOYMENT PROGRAM

Funding Recipients' Attestations for Cybersecurity and Supply Chain Risk Management



USTELECOM | THE BROADBAND ASSOCIATION

CONTENTS

BEAD Cybersecurity and Supply Chain Risk Management Attestation Guide for Small and Medium-Sized Entities

The Department of Commerce's Broadband Equity, Access, and Deployment (BEAD) Notice of Funding Opportunity (NOFO) requires that a prospective subgrantee have both a cybersecurity risk management plan and a supply chain risk management (SCRM) plan in place that is either operational or ready to be operationalized upon providing service. The BEAD NOFO also requires alignment with certain other guidelines and other requirements for a prospective subgrantee to be successful in applying for funding.

Section I of this document outlines the requirements for these cybersecurity and SCRM "attestations" in their entirety.

Section II provides a quick-reference list of resources referred to throughout.

To assist members bidding for contracts through the BEAD funding program, USTelecom provides two worksheet-style guides—the **BEAD Cybersecurity Attestation Guide** and the **BEAD Supply Chain Risk Management Attestation Guide**—that you can use as a practical tool for executive level discerning questions/statements for potential subgrantees to ensure their cybersecurity and supply chain risk management plans align to the BEAD NOFO requirements, including implementation tips and references to further NIST guidance where appropriate. In short, these worksheets are aimed at ensuring that your enterprise can attest to the fact that your plans satisfy the requirements outlined in Section I below.

Finally, we also provide for your reference in an Appendix **NIST's Cybersecurity Supply Chain Risk Assessment (C-SCRA) Template**, which serves as a supplemental reference to the BEAD Supply Chain Risk Management Attestation Worksheet.

If you have any questions regarding this guidance, please do not hesitate to contact Robert Mayer, Senior Vice President for Cybersecurity & Innovation at rmayer@ustelecom.org.

1. BEAD Program Overview

The Broadband Equity, Access, and Deployment (BEAD) Program, established by the Infrastructure Investment and Jobs Act (IIJA), is a federal funding opportunity which provides $42.45 billion in grants to Eligible Entities to expand high-speed internet access by funding broadband planning, deployment, mapping, equity, and adoption projects and activities. Eligible Entities for the program include all 50 states, Washington D.C., Puerto Rico, the U.S. Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

Each state, D.C., and P.R. will receive an initial allocation of $100 million—and $100 million will be divided equally among the United States Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands—to support planning efforts including building capacity in state broadband offices and outreach and coordination with local communities.[1]

The National Telecommunications and Information Administration (NTIA) is the agency within the U.S. Department of Commerce that administers the program. In its June 2022 Notice of Funding Opportunity, the following spending priorities[2] were established:

- Fiber connectivity directly to the end user.
- Unserved locations—those without access to 25-megabit-per-second (Mbps) download service and 3-Mbps uploads, commonly expressed as 25/3-Mbps service.
- Proposals that improve affordability to ensure that networks built using taxpayer dollars are accessible to all Americans.

While delivering affordable fiber connections to unserved areas takes precedence, "states may thereafter also apply funds to connecting underserved areas, which are those without access to 100/20-Mbps service; providing 1-gigabit-per-second symmetrical—meaning for both upload and download—connections to community anchor institutions such as libraries, schools, and hospitals; supporting digital skills training, workforce development, and provision of telehealth services; and promoting other broadband-related uses."[3]

To apply for funding, Eligible Entities must fulfill the requirements of The Broadband Equity, Access, and Deployment (BEAD) Notice of Funding Opportunity (NOFO).

2. BEAD Program Requirements under the NOFO

CYBERSECURITY ATTESTATION[4]

With respect to cybersecurity, prior to allocating any funds to a subgrantee, an Eligible Entity shall, at a minimum, require a prospective subgrantee to attest that:[5]

1. The prospective subgrantee has a cybersecurity risk management plan (the plan) in place that is either:

   A. operational, if the prospective subgrantee is providing service prior to the award of the grant; or

   B. ready to be operationalized upon providing service, if the prospective subgrantee is not yet providing service prior to the grant award.

   The plan reflects the latest version of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (currently Version 1.1) and the standards and controls set forth in Executive Order 14028 and specifies the security and privacy controls being implemented.

> *Disclaimer: No part of this guide constitutes legal advice and individual companies must check with state authorities to understand specific requirements for grant funding that may apply in their respective states and situations.*

What does it mean for a network service provider seeking BEAD grants to have a plan reflecting the latest version of the NIST Framework (Version 1.1)?

The bidder's plan should describe how it uses the NIST Framework to ensure confidentiality, integrity, and availability in the context of its provision of broadband services. It should identify specific standards, best practices, and guidelines in the NIST Framework that it has implemented.

The Framework organizes its core material into five functions—Identify, Protect, Detect, Respond, and Recover. In this guide, we address each of these functions tailored to an SMB perspective.

What does it mean for a network service provider seeking BEAD grants to have a plan reflecting standards and controls associated with EO 14028?

Consistent with EO 14028's guidance to federal agencies, a bidder's plan should describe to what extent it utilizes, in the context of its provision of broadband service, key principles associated with cloud security, zero trust architecture, secure software, and threat information sharing. While EO 14028 does not set forth controls or standards for organizations to implement, the bidder should describe whether it follows appropriate practices relevant to each of those areas in its cybersecurity risk management program.

Notably, the Cybersecurity Framework sets forth many specific standards, guidelines, and best practices that correspond to appropriate cloud security, zero trust architecture, secure software, and threat information sharing practices as outlined in EO 14028. Accordingly, bidders are encouraged to

describe how their use of the Cybersecurity Framework and/or their cybersecurity risk management program reflects the principles in EO 14028.

For example, an organization with strong authentication standards and controls as part of its implementation of the Cybersecurity Framework and/or cybersecurity risk management program could demonstrate that appropriate zero trust principles are reflected in its plan. Zero Trust Architecture is a relatively nascent concept that is still being fleshed out in multiple forums, and for which there currently do not exist specific standards and controls, so it would not be expected that a bidder would attest to having "implemented" that specific concept.

2. The plan will be reevaluated and updated on a periodic basis and as events warrant.

3. The plan will be submitted to the Eligible Entity prior to the allocation of funds. If the subgrantee makes any substantive changes to the plan, a new version will be submitted to the Eligible Entity within 30 days.

SUPPLY CHAIN RISK MANAGEMENT ("SCRM") ATTESTATION[6]

The Eligible Entity must provide a subgrantee's plan to NTIA upon NTIA's request. With respect to supply chain risk management (SCRM), prior to allocating any funds to a subgrantee, an Eligible Entity shall, at a minimum, require a prospective subgrantee to attest that:

1. The prospective subgrantee has a SCRM plan in place that is either:

   A. operational, if the prospective subgrantee is already providing service at the time of the grant; or

   B. ready to be operationalized, if the prospective subgrantee is not yet providing service at the time of grant award;

2. The plan is based upon the key practices discussed in the NIST publication NISTIR 8276, Key Practices in Cyber Supply Chain Risk Management: Observations from Industry and related SCRM guidance from NIST, including NIST 800-161, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations and specifies the supply chain risk management controls being implemented;

3. The plan will be reevaluated and updated on a periodic basis and as events warrant; and

4. The plan will be submitted to the Eligible Entity prior to the allocation of funds. If the subgrantee makes any substantive changes to the plan, a new version will be submitted to the Eligible Entity within 30 days. The Eligible Entity must provide a subgrantee's plan to NTIA upon NTIA's request.

An Eligible Entity also must ensure that, to the extent a BEAD subgrantee relies in whole or in part on network facilities owned or operated by a third party (e.g., purchases wholesale carriage on such facilities), obtain the above attestations from its network provider with respect to both cybersecurity and supply chain risk management practices.

3. Resources & References

- BEAD NOFO—*Broadband Equity, Access, and Deployment Program Notice of Funding Opportunity*
- Executive Order 14028—*Improving the Nation's Cybersecurity*
- NISTIR 8276—*Key Practices in Supply Chain Risk Management*
- NIST Cybersecurity Framework (currently Version 1.1)—*Framework for Improving Critical Infrastructure Cybersecurity*
- NIST SP 800-161—*Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*

BEAD Cybersecurity Attestation Worksheet

The BEAD Notice of Funding Opportunity (NOFO) requires that a prospective subgrantee have a cybersecurity risk management plan in place that is either operational or ready to be operationalized upon providing service. The plan must reflect the latest version of the NIST Cybersecurity Framework (currently Version 1.1) and the standards and controls set forth in Executive Order 14028. This plan must be reevaluated and updated on a periodic basis and as events warrant. This plan must be submitted to the Eligible Entity (i.e., State/Territory) prior to allocation of the funds and any substantive changes to the plan will also be submitted to the state/territory within 30 days.[7]

We have crafted the questions and statements below to guide you in ensuring your enterprise's cybersecurity plan covers the elements necessary to meet the requirements of the BEAD NOFO's cybersecurity risk management plan requirements outlined above.

The categories and questions below were developed to align with the NIST Cybersecurity Framework and Executive Order 14028, as required by the BEAD NOFO. They track the five Core Functions of the Framework: Identify, Protect, Detect, Respond, Recover.

Your enterprise should answer all questions below in detail (where applicable) and in the affirmative (for questions asking to "confirm") to successfully attest to BEAD cybersecurity requirements when applying for BEAD funding as a potential subgrantee. All references to "your enterprise" and "you" refer to the entity in question who will be considered the potential subgrantee for BEAD funding application purposes.

Your enterprise should ensure that this implementation guide is provided to personnel responsible for ensuring the cybersecurity requirements of the BEAD program are met, which may include internal risk management teams, C-suite executives with risk management responsibilities, and other leaders in your enterprise.

You should work through these questions to meet the initial attestation and implement a process for reevaluating on a regular basis. If and when answers change, an updated copy should be circulated to all interested parties with a point of contact to whom they can direct questions on the change in answers. If changes are substantive, re-submit the plan within 30 days to the state/territory.

1. Identify

A. What activities by your enterprise absolutely must continue to be viable?

IMPLEMENTATION TIP➔ Examples of such activities may include maintaining a website to retrieve payments; protecting customer/patient information securely; ensuring that the information your enterprise collects remains accessible and accurate.

B. What type of information does your enterprise collect and use? Where is this data located and how is it used?

IMPLEMENTATION TIP➔ It is particularly important to know where this information is stored and how it is used where contracts and external partners are engaged.

C. Confirm your enterprise keeps an inventory of the hardware and software in it. This inventory should be regularly updated.

IMPLEMENTATION TIP➔ An inventory can be as simple as a spreadsheet.

D. Confirm your enterprise's cybersecurity policies include roles and responsibilities.

IMPLEMENTATION TIP➔ These policies and procedures should clearly describe your expectations for how cybersecurity activities will protect your information and systems, and how they support critical enterprise processes. Cybersecurity policies should be integrated with other enterprise risk considerations (e.g., financial, reputational).

E. Confirm risk management processes are established and managed to ensure internal and external threats are identified, assessed, and documented in risk registers. Please confirm risk responses identified and prioritized, executed, and results monitored.

F. Specify the security and privacy controls being implemented.

2. Protect

A. Confirm your enterprise manages access to assets and information.

IMPLEMENTATION TIP➔ For example, your organization may create unique accounts for each employee and ensure that users only have access to information, computers, and applications that are needed for their jobs; authenticate users (e.g., passwords, multi-factor techniques) before they are granted access to information, computers, and applications; and tightly manage and track physical access to devices.

B. If your enterprise stores or transmits sensitive data, confirm you protect this data by encryption both while it is stored on computers as well as when it is transmitted to other parties.

IMPLEMENTATION TIP➔ Consider utilizing integrity checking to ensure only approved changes to the data have been made.

C. If your enterprise stores or transmits sensitive data, please confirm your enterprise deletes and/or destroys data when it is no longer needed or required for compliance purposes.

D. Confirm your enterprise conducts regular data backups.

IMPLEMENTATION TIP➔ Many operating systems have built-in backup capabilities; software and cloud solutions are also available that can automate the backup process. A good practice is to keep one frequently backed up set of data offline to protect it against ransomware.

E. Confirm that your enterprise protects its devices by (1) applying uniform configurations to devices and controlling changes to device configurations; (2) disabling device services or features not necessary to support mission critical functions; (3) ensuring there is a policy and that devices are securely disposed of.

IMPLEMENTATION TIP➔ Also consider installing host-based firewalls and other protections such as endpoint security products.

F. Confirm that your enterprise regularly updates both the operating system and applications installed on your computers and other devices to protect them from attack.

IMPLEMENTATION TIP➔ If possible, enable automatic updates. Consider using software tools to scan devices for additional vulnerabilities; remediate vulnerabilities with high likelihood and/or impact.

G. Confirm your enterprise regularly trains and retrains all users to ensure they are aware of enterprise cybersecurity policies and procedures and their specific roles and responsibilities as a condition of employment.

3. Detect

A. **Confirm that your enterprise has developed and tested processes and procedures for detecting unauthorized entities and actions on the networks and in the physical environment, including personnel activity. Staff should be aware of their roles and responsibilities for detection and related reporting both within your enterprise and to external governance and legal authorities.**

B. **Confirm you know the expected data flows for your enterprise. If you have contracted work to a cloud or managed service provider, please confirm that you have discussed with them how they track data flows and report, including unexpected events.**

> **IMPLEMENTATION TIP➔** If you know what and how data is expected to be used for your enterprise, you are much more likely to notice when the unexpected happens. Example: Unexpected data flows might include customer information being exported from an internal database and exiting the network.

C. **Confirm that your enterprise maintains and monitors logs.**

> **IMPLEMENTATION TIP➔** Logs are crucial to identify anomalies in your enterprise's computers and applications. These logs record events such as changes to systems or accounts as well as the initiation of communication channels. Consider using software tools that can aggregate these logs and look for patterns or anomalies from expected network behavior.

D. **Confirm that in the event a cybersecurity event is detected, your enterprise will work quickly and thoroughly to understand the breadth and depth of the impact and that you will seek help if needed.**

> **IMPLEMENTATION TIP➔** Communicating information on the event with appropriate stakeholders will help keep you in good stead in terms of partners, oversight bodies, and others (potentially including investors) and improve policies and processes.

4. Respond

A. **Confirm that response plans have been tested and that these response plans will be updated with lessons learned. This includes knowing of any legal reporting requirements or required information sharing.**

> **IMPLEMENTATION TIP➔** Testing the plan (and execution during an incident) inevitably will reveal needed improvements.

B. **Confirm that your enterprise's response plans and updates include all key stakeholders and external service providers.**

5. Recover

A. **Confirm that your recovery plans carefully account for what, how, and when information will be shared with various stakeholders so all interested parties receive the information they need but no inappropriate information is shared.**

B. **Confirm that your enterprise updates recovery plans with lessons learned.**

C. **Confirm you consider managing public relations and company reputation in developing recovery plans.**

IMPLEMENTATION TIP➔ One of the key aspects of recovery is managing the enterprise's reputation. When developing a recovery plan, consider how you will manage public relations so that your information sharing is accurate, complete, and timely—and not reactionary.

BEAD SCRM Attestation Worksheet

The BEAD Notice of Funding Opportunity (NOFO) requires that a prospective subgrantee have a supply chain risk management (SCRM) plan in place that is either operational or ready to be operationalized upon providing service. The plan must reflect the key practices discussed in NISTIR 8276 and include guidance from NIST, including NIST SP 800-161. This plan must be reevaluated and updated on a periodic basis and as events warrant. This plan must be submitted to the Eligible Entity (i.e., state/territory) prior to allocation of the funds and any substantive changes to the plan will also be submitted to the state/territory within 30 days.[8]

The questions and statements below are designed to guide you in ensuring your enterprise's SCRM plan covers the elements necessary to meet the requirements of the BEAD NOFO outlined above.

These categories and questions below were developed to capture the key practices considered in NISTIR 8276 and the Cybersecurity Supply Chain Risk Assessment (C-SCRA) found in NIST SP 800-161.

Your enterprise should answer all questions below in detail (where applicable) and in the affirmative (for questions asking to "confirm") to successfully attest to BEAD SCRM requirements when applying for BEAD funding as a potential subgrantee. All references to "your enterprise," "the organization," and "you" refer to the entity in question that will be considered the potential subgrantee for BEAD funding application purposes.

Your enterprise should ensure that this implementation guide is provided to personnel responsible for ensuring the supply chain requirements of the BEAD program are met, which may include internal risk management teams, C-suite executives with risk management responsibilities, procurement officials, and other leaders in your enterprise.

You should work through these questions to meet the initial attestation and implement a process for reevaluating on a regular basis. If and when answers change, an updated copy should be circulated to all interested parties with a point of contact to whom they can direct questions on the change in answers. If changes are substantive, re-submit the plan within 30 days to the state/territory.

1. Establish a Formal Cybersecurity Supply Chain Risk Management (C-SCRM) Program and Implement It Across the Organization

A. Confirm that you have established a formal C-SCRM program.

IMPLEMENTATION TIP➔ See NISTIR 8276 at 7: Smaller organizations may not need the structure required by larger organizations. For example, a small manufacturing organization may not need as many formal processes as a large technology company. (Examples include: "approved" and "banned" supplier lists; same policies used internally and with suppliers; increasing Executive Board or Executive Level involvement for establishing C-SCRM as a top business priority and to ensure proper oversight; establishing protocols for securely terminating supplier relationships to ensure all hardware containing acquirer's data has been properly disposed of and that risks of data leakage have been minimized.)

B. Specify the supply chain risk management controls your enterprise implements.

C. Do you have a Supply Chain Risk Council or Supply Chain Leadership Risk Council? If not, consider establishing such a group.

IMPLEMENTATION TIP➔ See NISTIR 8276 at 6: A number of organizations have established Supply Chain Risk Councils (or Supply Chain Leadership Risk Councils) that include executives from supply chain/procurement, information technology, cybersecurity, operations, legal, enterprise risk management (ERM), and other functional and leadership areas of the organization, depending on the organization's business and structure. These Councils proactively review relevant risks and risk mitigation plans, set priorities, direct sharing of best practices throughout the enterprise, and pilot initiatives. They also result in informal networks of leaders that facilitate trust and accountability in complex business environments. The benefit of Councils is the shared risk decision-making that ensures all perspectives are addressed.

D. Confirm you have a process to conduct a timely Supply Chain Risk Assessment as required in SP 800-161's Cybersecurity Supply Chain Risk Assessment (C-SCRA) template. The template is attached for your use with each third-party product, service, or supplier.

IMPLEMENTATION TIP➔ See NIST SP 800-161r1 at 218: The Cybersecurity Supply Chain Risk Assessment (C-SCRA) guides the review of any third-party product, service, or supplier that could present a cybersecurity risk to a procurer. Typically executed by C-SCRM PMOs at the operational level (Level 3), the C-SCRAC-SCRA considers available public and private information to perform a holistic assessment, including known cybersecurity risks throughout the supply chain, the likelihoods of their occurrence, and their potential impacts on an enterprise and its information and systems. As enterprises may be inundated with C-SCRAC-SCRAs and suppliers inundated with C-SCRAC-SCRA requests, the enterprise should evaluate the relative priority of its C-SCRAC-SCRAs as an influencing factor on the rigor of the CSCRAC-SCRA. This template is provided only as an example. Enterprises must tailor the content to align with their Level 1 and Level 2 risk postures. The execution of C-SCRAC-SCRA is perhaps the most visible and time-consuming component of C-SCRM operations and must therefore be designed for efficient execution at scale with dedicated support resources, templated workflows, and automation wherever possible. ***We provide NIST's C-SCRA Template as an Appendix to this document.***

E. State the roles and responsibilities for the C-SCRA policies and its key contributors. Include the role and name of each individual or group, as well contact information where necessary (e.g., enterprise affiliation, address, email address, phone no.).

IMPLEMENTATION TIP→ See NIST SP 800-161r1 at 231:

The enterprise's C-SCRM lead shall:

- Maintain C-SCRA policies, procedures, and scoring methodologies,
- Perform C-SCRA standard operating procedures,
- Liaise with requestors seeking to procure a product, service, or supplier, and
- Report C-SCRA results to leadership to help inform enterprise risk posture.

Each requestor shall:

- Complete C-SCRA request forms and provide all required information,
- Address any information follow-up requests from the C-SCRM PMO resource completing the C-SCRA, and
- Adhere to any stipulations or mitigations mandated by the C-SCRM PMO following approval of a C-SCRA request.

F. Define the required frequency for updating the C-SCRA template. Maintain a table of revisions to enforce version control. C-SCRA templates are living documents that must be updated and communicated to all appropriate individuals (e.g., staff, contractors, and suppliers).

IMPLEMENTATION TIP→ See NIST SP 800-161r1 at 231-32: The enterprise's C-SCRA template must be reviewed on an annual basis, at a minimum, since changes to laws, policies, standards, guidelines, and controls are dynamic and evolving. Additional criteria that may trigger interim revisions include:

- A change of policies that impact the C-SCRA template,
- Significant C-SCRM events,
- The introduction of new technologies,
- The discovery of new vulnerabilities,
- Operational or environmental changes,
- Shortcomings in the C-SCRA template,
- A change of scope, and
- Other enterprise-specific criteria.

2. Know and Manage Critical Components and Suppliers

A. Identify and prioritize critical missions, assets, systems, processes, and data and then identify suppliers that either have access to or provide infrastructure for critical assets, systems, processes, and data.

B. Identify critical suppliers which, if disrupted, would create a negative business impact on the organization.

IMPLEMENTATION TIP➔ See NISTIR 8276 at 8: Several criteria can be used to determine component and supplier criticality:

- Revenue contribution of suppliers
- Whether a supplier processes critical data belonging to the acquirer, such as regulated data (e.g., PII, PHI) or intellectual property
- Volume of data a supplier has access to or hosts
- Whether a supplier has access to the acquirer's system and network infrastructure
- Whether a supplier can become an attack vector by being compromised and allowing threat actors access to the acquirer
- For technology companies, whether a supplier can become an attack vector for the technology company's products or services delivered to customers

NIST has made available a free tool that helps identify the impact of suppliers to the organization. The tool is described in NISTIR 8272, Impact Analysis Tool for Interdependent Cyber Supply Chain Risks, along with instructions on how to use it [NISTIR 8272]. NISTIR 8179, Criticality Analysis Process Model, provides a comprehensive methodology for determining project and product criticality that can be used as an input in determining system, component, and supplier criticality [NISTIR 8179]. The Business Impact Analysis (BIA) described in NIST SP 800-34, Rev. 1, Contingency Planning Guide for Federal Information Systems, can also be used to determine supplier criticality [SP 800-34]. The Business Continuity Planning booklet published by the FFIEC (Federal Financial Institutions Examination Council) provides a process and list of considerations that can be adapted to determine supplier criticality [FFIEC BCP].

3. Understand the Organization's Supply Chain

A. Confirm the appropriate people understand the organization's supply chain, including any layers of sub-suppliers.

IMPLEMENTATION TIP➔ See NISTIR 8276 at 9: Today's supply chains are extended, extensive, and include multiple organizations across the globe. In this environment, the risks may stem from suppliers' connectivity to their suppliers, component sourcing for hardware and software suppliers, technologies shared upstream and downstream within supply chains, and processes and people within those supply chains. Best practice organizations establish real-time visibility into the production processes of their outsourced manufacturers with the capacity to capture not only defect rates but causes of failure and, therefore, prevent a supplier's ability to shortcut testing requirements before shipment. This includes the use of software and hardware component inventory as well as tools and methods to audit provenance claims at any point in the supply chain. Such visibility and transparency reduce the risk of tampering and counterfeiting and improve the security, and ultimately the quality, of the resulting products. Additionally, best practice organizations have insight into how their suppliers vet their personnel, who they are outsourcing to, and who has access to the acquirer's data.

4. Closely Collaborate With Key Suppliers

A. **Does your organization have close relationships with its suppliers up to and including shared ecosystems between acquirers and suppliers? If not, consider establishing such close relationships.**

IMPLEMENTATION TIP➔ NISTIR 8276 at 9-10: Increasingly, organizations are treating their suppliers as members of their ecosystem and closely collaborating in a variety of ways:

- Acquirers maintain close working relationships through frequent visits and communications.
- Acquirers mentor and coach suppliers on C-SCRM and actively help suppliers improve their cybersecurity and supply chain practices.
- Acquirers and suppliers invest in common solutions.
- Acquirers require the use of the same standards within the acquirer organizations and by suppliers, thereby simplifying communications about cybersecurity risk and mitigations and helping to achieve a uniform level of quality throughout the ecosystem.

The sophistication and level of formality of acquirer-supplier relationships increase with the maturity of the C-SCRM practices. For example, smaller businesses establish and maintain close relationships with their key suppliers by conducting frequent visits, phone calls, and other forms of informal communication. Larger and more mature organizations use more documented processes and procedures and hold multiple formal meetings with their suppliers.

5. Include Key Suppliers In Resilience and Improvement Activities

A. **Does your organization have resiliency plans in place? If not, consider establishing such plans.**

IMPLEMENTATION TIP➔ See NISTIR 8276 at 10: Threat actors actively target acquirers through suppliers. In addition to cybersecurity risks, there are environmental risks, such as severe weather, and risks associated with geopolitical unrest, that continually threaten to disrupt the supply chain. Incidents will happen to even the most mature organizations, which makes resiliency planning essential. Mature organizations include their critical suppliers, products, and assets in their contingency planning, incident response, and disaster recovery. These organizations test such plans with key stakeholders, including suppliers, to guarantee the readiness of all involved parties and the effectiveness of the plans. This ensures that critical procedures and protocols are established and well-understood ahead of any significant event.

Resilience and improvement activities include:

- Rules and protocols for information sharing between acquirers and suppliers, sometimes within larger critical infrastructure sector ecosystems
- Joint development, review, and revision of incident response, business continuity, and disaster recovery plans
- Protocols for communicating vulnerabilities and incidents
- Responsibilities for responding to cybersecurity incidents
- Coordinated communication methods and protocols
- Coordinated restoration and recovery procedures
- Collaborative processes to review lessons learned
- Updates of coordinated response and recovery plans based on lessons learned

More mature acquirers have formal continuous improvement processes that include collecting lessons learned from supply chain incidents; sharing potential improvements throughout the ecosystem; incorporating results into planning, response, and recovery processes; and sharing them with appropriate organizations throughout the enterprise. This process includes stakeholders from the organization and suppliers to ensure that identified risks are remediated.

6. Assess and Monitor Throughout the Supplier Relationship

A. **Confirm that you assess supplier controls on a regular basis. The frequency and robustness of the assessments should be established based on supplier criticality. Critical suppliers should be assessed more frequently, and more extensive assessment methods should be used to determine if there are any changes in risk.**

IMPLEMENTATION TIP➔ See NISTIR 8276 at 11: A supplier assessment conducted prior to bringing a supplier on board is a snapshot in time that becomes obsolete before it is completed. Assessing supplier controls on a regular basis helps manage cyber supply chain risks by determining whether agreed-upon requirements and controls are being met, identifying improvements that may be required, and monitoring the completion of those improvement actions.

7. Plan For the Full Life Cycle

A. **Confirm you have multiple practices in place for managing the risk of unexpected supply chain interruptions.**

IMPLEMENTATION TIP➔ See NISTIR 8276 at 12: When organizations put technical solutions into their infrastructures, they expect those solutions to continue working for as long as they are needed by the organization. However, organizations should plan for unexpected interruptions to the supply chain to ensure business continuity. Examples of such interruptions include suppliers stopping support of obsolete hardware and software, discontinuing production of hardware components, or adopting a significant change of business direction caused by acquisition or changes in supplier ownership or management. Organizations should deploy a variety of practices to manage this particular risk, including purchasing reserve quantities of critical components and establishing relationships with approved resellers that are likely to stay in business.

APPENDIX

NIST Cybersecurity Supply Chain Risk Assessment (C-SCRA) Template

The following template is excerpted from NIST SP 800-161 Rev.1.

4. CYBERSECURITY SUPPLY CHAIN RISK ASSESSMENT TEMPLATE

The Cybersecurity Supply Chain Risk Assessment (C-SCRA)[9] guides the review of any third-party product, service, or supplier[10] that could present a cybersecurity risk to a procurer. The objective of the C-SCRA template is to provide a toolbox of questions that an acquirer can choose to use or not use depending on the controls selected. Typically executed by C-SCRM PMOs at the operational level (Level 3), the C-SCRAC-SCRA considers available public and private information to perform a holistic assessment, including known cybersecurity risks throughout the supply chain, the likelihoods of their occurrence, and their potential impacts on an enterprise and its information and systems. As enterprises may be inundated with C-SCRAC-SCRAs and suppliers inundated with C-SCRAC-SCRA requests, the enterprise should evaluate the relative priority of its C-SCRAC-SCRAs as an influencing factor on the rigor of the C-SCRAC-SCRA.

As with the other featured templates, the below C-SCRAC-SCRA is provided only as an example. Enterprises must tailor the below content to align with their Level 1 and Level 2 risk postures. The execution of C-SCRAC-SCRA is perhaps the most visible and time-consuming component of C-SCRM operations and must therefore be designed for efficient execution at scale with dedicated support resources, templated workflows, and automation wherever possible. Federal agencies should refer to Appendix E for additional guidance concerning supply chain risk assessments.

4.1. C-SCRM Template

4.1.1. Authority and Compliance

List the laws, executive orders, directives, regulations, policies, standards, and guidelines that govern C-SCRAC-SCRA execution.

SAMPLE TEXT

- Legislation o Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE) Technology of 2018
- Policies o [Enterprise name] C-SCRA Standard Operating Procedures o [Enterprise name] C-SCRA Risk Assessment Factors o [Enterprise name] C-SCRA Criticality Assessment Criteria
- Guidelines o NIST 800-53, Rev. 5: PM-30, RA-3, SA-15, SR-5 o NIST 800-37, Rev. 2 o NIST 800-161, Rev. 1: Appendix C o ISO 28001:2007

4.1.2. Description

Describe the purpose and scope of the C-SCRA template and reference the enterprise commitment to C-SCRM and mandate to perform C-SCRAs as an extension of that commitment. Outline the template's relationship to enterprise risk management principles, frameworks, and practices. This may include providing an overview of the enterprise's C-SCRA processes, standard operating procedures, and/or criticality designations that govern the usage of this template.

Reinforce the business case for executing C-SCRA by highlighting the benefits of reducing expected loss from adverse supply chain cybersecurity events, as well as the C-SCRM PMO's role in efficiently executing these assessments at scale.

Provide an overview of the enterprise's boundaries, systems, and services within the scope of the C-SCRAs.

List the contact information and other resources that readers may access in order to further engage with the C-SCRA process.

SAMPLE TEXT

This C-SCRA is intended to fairly and consistently evaluate risks posed to the [enterprise] via third parties that hold the potential for harm or compromise as a result of cybersecurity risks. Cybersecurity risk in the supply chain includes exposures, threats, and vulnerabilities associated with the products and services traversing the supply chain, as well as the exposures, threats, and vulnerabilities to the supply chain and its suppliers.

The C-SCRA template provides tactical guidelines for the C-SCRM PMO to review cybersecurity risk in the supply chain and ensure that C-SCRAs are appropriately, efficiently, and effectively carried out in line with enterprise mandates.

Requestors seeking to introduce third-party products, services, or suppliers into enterprise boundaries should familiarize themselves with the following template. This will ensure that requestors can provide the requisite information to the C-SCRM PMO to ensure timely execution of C-SCRAs and are otherwise aligned with adherence to the steps of the C-SCRA.

The C-SCRA process contains five primary steps, as outlined in the below template:[11]

1. Information Gathering and Scoping Analysis
2. Threat Analysis
3. Vulnerability Analysis
4. Impact Analysis
5. Risk Response Analysis

To learn more about the C-SCRA process and/or submit an assessment request to the C-SCRM PMO, please go to [enterprise's intranet page] or contact [C-SCRM PMO email].

4.1.3. Information Gathering and Scoping Analysis

Define the purpose and objectives for the requested C-SCRA and outline the key information required to appropriately define the system, operations, supporting architecture, and boundaries. Provide key questions to requestors to facilitate the collection and analysis of this information. The C-SCRM PMO will then use this information as a baseline for subsequent analyses and data requests.

SAMPLE TEXT

TABLE D-13: INFORMATION GATHERING AND SCOPING ANALYSIS

SUPPLY CHAIN RISK MANAGEMENT ASSESSMENT SCOPING QUESTIONNAIRE		
SECTION 1: REQUEST OVERVIEW	**PROVIDE RESPONSE:**	**RESPONSE PROVIDED BY:**
Requestor Name		Acquirer
C-SCRA Purpose and Objective		Acquirer
System Description		Acquirer
Architecture Overview		Acquirer
Boundary Definition		Acquirer
Date of Assessment		Acquirer
Assessor Name		Acquirer
SECTION 2: PRODUCT/SERVICE INTERNAL RISK OVERVIEW		
What % of this supplier's sales of this product/service does your enterprise consume?		Acquirer or Supplier
How widely used is or will the product or service be in your enterprise?		Acquirer
Is the product/service manufactured in a geographic location that is considered an area of geopolitical risk for your enterprise based on its primary area of operation (e.g., in the United States)?		Acquirer or Supplier
Is the product manufactured or developed in a country identified as a foreign adversary or country of special concern?		Acquirer

SUPPLY CHAIN RISK MANAGEMENT ASSESSMENT SCOPING QUESTIONNAIRE		
Would switching to an alternative supplier for this product or service constitute significant cost or effort for your enterprise?		Acquirer
Does your enterprise have an existing relationship with another supplier for this product/service?		Acquirer
How confident is your enterprise that they will be able to obtain quality products/services regardless of major supply chain disruptions, both human and natural?		Acquirer
Does your enterprise maintain a reserve of this product/service?		Acquirer
Is the product/service fit for purpose? (i.e., capable of meeting objectives or service levels)?		Acquirer
Does the product/service perform an essential security function? If so, please describe.		Acquirer
Does the product/service have root access to IT networks, OT systems, or sensitive platforms?		Acquirer
Can compromise of the product/service lead to system failure or severe degradation?		Acquirer
In the event of compromise leading to system failure or severe degradation, is there a known independent reliable mitigation?		Acquirer
Will/does the product/service connect to a platform that is provided to customers by your enterprise?		Acquirer
Will/does the product/service transmit, generate, maintain, or process high value data (e.g., PII, PHI, PCI)?		Acquirer
Will/does the product/service have access to systems that transmit, generate, maintain or process high value data (e.g., PII, PHI, PCI)?		Acquirer
Will/does the supplier require physical access to the company's facilities as a result of its provision of the product/service?		Acquirer
Based on holistic consideration of the above responses, how critical is this product/service to your enterprise (i.e., critical, high, moderate, low)?		Acquirer

SUPPLY CHAIN RISK MANAGEMENT ASSESSMENT SCOPING QUESTIONNAIRE		
SECTION 3: SUPPLIER OVERVIEW		
Have you identified the supplier's critical suppliers?		Supplier
Did you verify the supplier ownership, whether foreign and domestic?		Supplier
If the supplier uses distributors, did you investigate them for potential risks?		Supplier
Is the supplier located in the United States?		Supplier
Does the supplier have personnel and/or professional ties (including its officers, directors, or similar officials, employees, consultants, or contractors) with any foreign government?		Supplier
Is there foreign ownership, control, or influence (FOCI) over the supplier or any business entities involved in the supply chain? If so, is the FOCI from a foreign adversary of the United States or country of concern?		Supplier
Do the laws and regulations of any foreign country in which the supplier has headquarters, research development, manufacturing, testing, packaging, distribution, or service facilities or other operations require the sharing of technology or data with that foreign country?		Supplier
Has the supplier declared where replacement components will be purchased from?		Supplier
Have the owners and locations of all of the suppliers, subcontractors, and sub-tier suppliers been identified and validated?		Supplier
Does the supplier employ the use of threat scenarios to inform the vetting of sub-tier suppliers?		Supplier
Does the supplier have documents that track part numbers to manufacturers?		Supplier
Can the supplier provide a list of who they procure hardware and software from that is utilized in the performance of the contract?		Supplier

SUPPLY CHAIN RISK MANAGEMENT ASSESSMENT SCOPING QUESTIONNAIRE		
Does the supplier have counterfeit controls in place?		Supplier
Does the supplier safeguard key program information that may be exposed through interactions with other suppliers?		Supplier
Does the supplier perform reviews and inspections and have safeguards to detect or avoid counterfeit equipment, tampered hardware or software (HW/SW), vulnerable HW/SW, and/or operations security leaks?		Supplier
Does the supplier use industry standard baselines (e.g., CIS, NES) when purchasing software?		Supplier
Does the supplier comply with regulatory and legislative mandates?		Supplier
Does the supplier have procedures for secure maintenance and upgrades following deployment?		Supplier
SECTION 4: POLICIES AND PROCEDURES		
Does the supplier have definitive policies and procedures that help minimize supply chain risk, including subsidiary sourcing needs?		Supplier
Does the supplier define and manage system criticality and capabilities?		Supplier
Does everyone associated with the procurement (e.g., supplier, C-SCRM PMO) understand the potential threats to and risks in the subject supply chain?		Supplier
What is the citizenship of all engaged personnel? If required, are all engaged personnel US citizens?		Supplier
Does the supplier have “insider threat” controls in place?		Supplier
Does the supplier verify and monitor all personnel who interact with the subject product, system, or service to know if they pose a threat?		Supplier
Does the supplier use, record, and track risk mitigation activities throughout the life cycle of the product, system, or service?		Supplier

SUPPLY CHAIN RISK MANAGEMENT ASSESSMENT SCOPING QUESTIONNAIRE		
Have all of the supplier's personnel signed non-disclosure agreements?		Supplier
Does the supplier allow its personnel or suppliers to remotely access environments?		Supplier
SECTION 5: LOGISTICS (IF APPLICABLE)		
Does the supplier have documented tracking and version controls in place?		Supplier
Does the supplier analyze events (environmental or human-made) that could interrupt their supply chain?		Supplier
Are the supplier's completed parts controlled so that they are never left unattended or exposed to tampering?		Supplier
Are the supplier's completed parts locked up?		Supplier
Does the supplier have a process that ensures integrity when ordering inventory from their supplier?		Supplier
Is the supplier's inventory periodically inspected for exposure or tampering?		Supplier
Does the supplier have secure material destruction procedures for unused and scrap parts procured from their supplier?		Supplier
Is there a documented chain of custody for the deployment of products and systems?		Supplier
SECTION 6: SOFTWARE DESIGN AND DEVELOPMENT (IF APPLICABLE)		
Is the supplier familiar with all of their suppliers that will work on the design of the product/system?		Supplier and Manufacturer
Does the supplier align its SDLC to a secure software development standard (e.g., Microsoft Security Development Life Cycle)?		Supplier and Manufacturer
Does the supplier perform all development onshore?		Supplier and Manufacturer
Do only United States citizens have access to development environments?		Supplier and Manufacturer

SUPPLY CHAIN RISK MANAGEMENT ASSESSMENT SCOPING QUESTIONNAIRE		
Does the supplier provide cybersecurity training to its developers?		Supplier and Manufacturer
Does the supplier use trusted software development tools?		Supplier and Manufacturer
Is the supplier using trusted information assurance controls to safeguard the development environment (e.g., secure network configurations, strict access controls, dynamic/static vulnerability management tools, penetration testing)?		Supplier and Manufacturer
Does the supplier validate open source software prior to use?		Supplier and Manufacturer
Are the supplier's software compilers continuously monitored?		Supplier and Manufacturer
Does the supplier have codified software test and configuration standards?		Supplier and Manufacturer
SECTION 7: PRODUCT- OR SERVICE-SPECIFIC SECURITY (IF APPLICABLE, ONE QUESTIONNAIRE PER PRODUCT/SERVICE)		
Name of Product or Service		Manufacturer
Product Type (i.e., hardware, software, service)		Manufacturer
Description of Product or Service		Manufacturer
Part Number (if applicable)		Manufacturer
Does the manufacturer implement formal enterprise roles and governance responsible for the implementation and oversight of secure engineering across the development or manufacturing process for product offerings?		Manufacturer
Does the manufacturer have processes for product integrity that conform to standards such as ISO 27036 or SAE AS6171?		Manufacturer
Is the product compliant with Federal Information Processing Standards (FIPS) 140-2? If yes, please provide the FIPS level.		Manufacturer
Does the manufacturer document and communicate security control requirements for your hardware, software, or solution offering?		Manufacturer

SUPPLY CHAIN RISK MANAGEMENT ASSESSMENT SCOPING QUESTIONNAIRE		
Has the manufacturer received fines or sanctions from any governmental entity or regulatory body in the past year related to delivery of the product or service? If yes, please describe.		Manufacturer
Has the manufacturer experienced litigation claims over the past year related to the delivery of the product or service? If yes, please describe.		Manufacturer
Does the manufacturer provide a bill of materials (BOM) for the products, service, or components, including all logic-bearing (e.g., readable, writable, programmable) hardware, firmware, and software?		Manufacturer
For hardware components included in the product or service offering, does the supplier only buy from original equipment manufacturers or licensed resellers?		Supplier
Does the manufacturer have a policy or process to ensure that none of your suppliers or third-party components are on any banned list?		Manufacturer
How does the manufacturer prevent malicious and/or counterfeit IP components in their product offerings or solutions?		Manufacturer
Does the manufacturer manage the integrity of IP for its products or service offerings?		Manufacturer
How does the manufacturer assess, prioritize, and remediate reported product or service vulnerabilities?		Manufacturer
How does the manufacturer ensure that product or service vulnerabilities are remediated in a timely period to reduce the window of opportunity for attackers?		Manufacturer
Does the manufacturer maintain and manage a Product Security Incident		Manufacturer
Reporting and Response program (PSRT)?		Manufacturer
What is the manufacturer's process for ensuring that customers and external entities (such as government agencies) are notified of an incident when their product or service is impacted?		Manufacturer

4.1.4. Threat Analysis

Define threat analysis as well as the criteria that will be utilized to assess the threat of the product, service, or supplier. Include a rubric with categorical definitions to encourage the transparency of assessment results.

SAMPLE TEXT

The C-SCRA threat analysis evaluates and characterizes the level of threat to the integrity, trustworthiness, and authenticity of the product, service, or supplier as described below. This analysis is based on a threat actor's capability and intent to compromise or exploit the product, service, or supplier being introduced into the supply chain. Following completion of the analysis, one of the following threat levels is assigned:

- **Critical:** Information indicates that an adversarial or non-adversarial threat is imminent (e.g., an adversary is actively engaged in subversion, exploitation, or sabotage of the product, service, or supplier).
- **High:** Information indicates that an adversarial or non-adversarial threat is imminent (e.g., significant drought in the geographical area combined with location characteristics of the asset yields high potential for forest fires).
- **Moderate:** Information indicates that an adversarial or non-adversarial threat has an average potential to impact or target the enterprise (e.g., a specific adversarial threat exists but lacks either the capability or the intent to engage in subversion, exploitation or sabotage of the product, service, or supplier).
- **Low:** Information indicates that adversarial or non-adversarial threats are non-existent, unlikely, or have below average potential to impact or target the enterprise (e.g., adversarial threats lack both the capability and the intent to engage in subversion, exploitation, or sabotage of the product, service, or supplier).

To appropriately assign the above threat analysis designation, C-SCRM PMOs and requestors should leverage the Information Gathering and Scoping questionnaire to coordinate the collection of information related to the product, service, or supplier's operational details, ownership structure, key management personnel, financial information, business ventures, government restrictions, and potential threats. Additional investigations of the aforementioned topics should be performed if red flags are observed during initial data collection.

4.1.5. Vulnerability Analysis

Define vulnerability analysis and the criteria that will be utilized to assess the vulnerability of the product, service, or supplier being assessed. Include a rubric with categorical definitions to encourage transparency behind assessment results.

SAMPLE TEXT

The C-SCRA vulnerability analysis evaluates and then characterizes the vulnerability of the product, service, or supplier throughout its life cycle and/or engagement. The analysis includes an assessment of the ease of exploitation by a threat actor with moderate capabilities. This analysis is based on a threat

actor's capability and intent to compromise or exploit the product, service, or supplier being introduced into the supply chain. Following completion of the analysis, one of the following threat levels is assigned:

- **Critical:** The product, service, or supplier contains vulnerabilities or weaknesses that are wholly exposed and easily exploitable.
- **High:** The product, service, or supplier contains vulnerabilities or weaknesses that are highly exposed and reasonably exploitable.
- **Moderate:** The product, service, or supplier contains vulnerabilities or weaknesses that are moderately exposed and difficult to exploit.
- **Low:** The product, service, or supplier contains vulnerabilities and weaknesses with limited exposure and are unlikely to be exploited.

To appropriately assign the above vulnerability analysis designation, C-SCRM PMOs and requestors should coordinate the collection of information related to the product, service, or supplier's operational details, exploitability, service details, attributes of known vulnerabilities, and mitigation techniques.

4.1.6. Impact Analysis

Define impact analysis and the criteria that will be utilized to assess the criticality of the product, service, or supplier being assessed. Include a rubric with categorical definitions to encourage the transparency of assessment results.

SAMPLE TEXT

The C-SCRA impact analysis evaluates and then characterizes the impact of the product, service, or supplier throughout its life cycle and/or engagement. The analysis includes an end-to-end functional review to identify critical functions and components based on an assessment of the potential harm caused by the probable loss, damage, or compromise of a product, material, or service to an enterprise's operations or mission. Upon completion of the analysis, one of the following impact levels is assigned:

- **Critical:** The product, service, or supplier's failure to perform as designed would result in a total enterprise failure or a significant and/or unacceptable level of degradation of operations that could only be recovered with exceptional time and resources.
- **High:** The product, service, or supplier's failure to perform as designed would result in severe enterprise failure or a significant and/or unacceptable level of degradation of operations that could only be recovered with significant time and resources.
- **Moderate:** The product, service, or supplier's failure to perform as designed would result in serious enterprise failure that could be readily and quickly managed with no long-term consequences.
- **Low:** The product, service, or supplier's failure to perform as designed would result in few adverse effects on the enterprise, and those effects could be readily and quickly managed with no long-term consequences.

To appropriately assign the above impact analysis designation, C-SCRM PMOs and requestors should coordinate the collection of information related to the enterprise's critical functions and components, the identification of the intended user environment for the product or service, and supplier information.

4.1.7. Risk Response Analysis

Define risk analysis and the criteria that will be utilized to assess the scoring of the product or service being assessed. Include a rubric with categorical definitions to encourage the transparency of assessment results.

SAMPLE TEXT

The C-SCRA risk exposure reflects a combined judgement based on likelihood and impact analyses. The likelihood analysis is scored via a combination of the aforementioned threat and vulnerability analysis score, as outlined in the figure below.

LIKELIHOOD LEVEL					
THREAT	VULNERABILITY				
		LOW	MODERATE	HIGH	CRITICAL
	CRITICAL	Moderately Likely	Highly Likely	Very Likely	Very Likely
	HIGH	Moderately Likely	Highly Likely	Highly Likely	Very Likely
	MODERATE	Unlikely	Moderately Likely	Highly Likely	Highly Likely
	LOW	Unlikely	Unlikely	Moderately Likely	Moderately Likely

FIG. D-2: EXAMPLE LIKELIHOOD DETERMINATION

The C-SCRA risk exposure is then aggregated based on that likelihood score and the impact score. If multiple vulnerabilities are identified for a given product or service, each vulnerability shall be assigned a risk level based on its likelihood and impact.

OVERALL RISK EXPOSURE					
LIKELIHOOD (THREAT AND VULNERABILITY)	IMPACT				
		LOW	MODERATE	HIGH	CRITICAL
	VERY LIKELY	Moderate	High	Critical	Critical
	HIGHLY LIKELY	Moderate	Moderate	High	Critical
	MODERATELY LIKELY	Low	Moderate	High	High
	UNLIKELY	Low	Low	Moderate	High

FIG. D-3: EXAMPLE RISK EXPOSURE DETERMINATION

The aforementioned risk analyses and scoring provide measures by which the enterprise determines whether or not to proceed with procurement of the product, service, or supplier. Decisions to proceed must be weighed against the risk appetite and tolerance across the tiers of the enterprise, as well as the mitigation strategy that may be put in place to manage the risks as a result of procuring the product, service, or supplier.

4.1.8. Roles and Responsibilities

State those responsible for the C-SCRA policies, as well as its key contributors. Include the role and name of each individual or group, as well contact information where necessary (e.g., enterprise affiliation, address, email address, and phone number).

SAMPLE TEXT

The C-SCRM PMO shall:

- Maintain C-SCRA policies, procedures, and scoring methodologies,
- Perform C-SCRA standard operating procedures,
- Liaise with requestors seeking to procure a product, service, or supplier, and
- Report C-SCRA results to leadership to help inform enterprise risk posture.

Each requestor shall:

- Complete C-SCRA request forms and provide all required information,
- Address any information follow-up requests from the C-SCRM PMO resource completing the C-SCRA, and
- Adhere to any stipulations or mitigations mandated by the C-SCRM PMO following approval of a C-SCRA request.

4.1.9. Definitions

List the key definitions described within the policy and provide enterprise-specific context and examples where needed.

SAMPLE TEXT

- Procurement: The process of obtaining a system, product, or service.

4.1.10. Revision and Maintenance

Define the required frequency for updating the C-SCRA template. Maintain a table of revisions to enforce version control. C-SCRA templates are living documents that must be updated and communicated to all appropriate individuals (e.g., staff, contractors, and suppliers).

SAMPLE TEXT

The enterprise's C-SCRA template must be reviewed on an annual basis, at a minimum, since changes to laws, policies, standards, guidelines, and controls are dynamic and evolving. Additional criteria that may trigger interim revisions include:

- A change of policies that impact the C-SCRA template,
- Significant C-SCRM events,
- The introduction of new technologies,
- The discovery of new vulnerabilities,

- Operational or environmental changes,
- Shortcomings in the C-SCRA template,
- A change of scope, and
- Other enterprise-specific criteria.

SAMPLE TEXT

TABLE D-14: VERSION MANAGEMENT TABLE

VERSION NUMBER	DATE	DESCRIPTION OF CHANGE/REVISION	SECTION/PAGES AFFECTED	CHANGES MADE BY NAME/TITLE/ENTERPRISE

Endnotes

1 https://broadbandusa.ntia.doc.gov/resources/grant-programs

2 https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2023/01/what-states-need-to-know-about-federal-bead-funding-for-high-speed-internet-expansion

3 https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2023/01/what-states-need-to-know-about-federal-bead-funding-for-high-speed-internet-expansion

4 *See* BEAD NOFO at 70.

5 As the entity applying for funding, you are the "prospective subgrantee." This means that your entity must attest to each of the enumerated provisions. See BEAD NOFO at 15 (defining "subgrantee").

6 BEAD NOFO at 70-71

7 The "Eligible Entity" is the entity offering you the funding—specifically, any state of the United States, the District of Columbia, Puerto Rico, American Samoa, Guam, the U.S. Virgin Islands, and the Commonwealth of the Northern Mariana Islands or, in the case of an application failure, a political subdivision or consortium of political subdivisions that is serving as a Substitute Entity.

8 The "Eligible Entity" is the entity offering you the funding—specifically, any state of the United States, the District of Columbia, Puerto Rico, American Samoa, Guam, the U.S. Virgin Islands, and the Commonwealth of the Northern Mariana Islands or, in the case of an application failure, a political subdivision or consortium of political subdivisions that is serving as a Substitute Entity.

9 For the purposes of this document, the expression "cybersecurity supply chain risk assessment" should be considered equivalent to "supply chain risk assessment" in an effort to harmonize terminology.

10 A supplier may also refer to a source, as defined in the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE) Technology of 2018.

11 .See Appendix D's "Assess" section for the methodological principles and guidance that underpin these steps