DELIVER UNCOMPROMISED: SUPPLY CHAIN RISK MANAGEMENT

OUR NATIONAL DEFENSE IS LARGELY DEPENDENT UPON TECHNOLOGIES AND CAPABILITIES DEVELOPED AND MANUFACTURED BY OUR DEFENSE INDUSTRIAL BASE. TODAY, THE DEFENSE INDUSTRIAL BASE IS UNDER ATTACK. OUR ADVERSARIES ARE STEALING VAST AMOUNTS OF CRITICAL TECHNOLOGY THAT JEOPARDIZE OUR MISSION READINESS, THE SAFETY AND SECURITY OF OUR WARFIGHTERS, AND THE SECURITY OF OUR CITIZENRY. ENSURING A MORE CAPABLE, RESILIENT, AND INNOVATIVE DEFENSE REQUIRES THAT CAPABILITIES DEVELOPED AND PRODUCED BY THE DEFENSE INDUSTRIAL BASE ARE DELIVERED TO THE WARFIGHTER UNCOMPROMISED. EFFECTIVE SUPPLY CHAIN RISK MANAGEMENT (SCRM) CAN MITIGATE THESE RISKS AND ENSURE THAT DOD TECHNOLOGY IS DELIVERED UNCOMPROMISED.

WHAT IS A SUPPLY CHAIN?

WHAT ARE THE THREATS TO MY SUPPLY CHAIN?

HOW CAN RISK MANAGEMENT PROTECT MY SUPPLY CHAIN?

Can you answer these questions?
Do you know what the answers mean?

Click here to access the Supply Chain Risk Management Self-Assessment Tool

SUPPLY CHAIN RISK MANAGEMENT SELF-ASSESSMENT

- Do you verify company ownership? Confirm U.S. ownership?
- If you use distributors, do you investigate them for potential threats?
- Have you identified where additional repair parts will be purchased?
- Are all sub-contractors and suppliers located onshore?
- Does the program office vet suppliers for threat scenarios?
- Do you have documents which track part numbers to manufacturers?
- Can you provide a list of who you purchased your COTS software from?
- Do you have an awareness regarding the likelihood of counterfeits?
- Do you safeguard key program information that may be exposed through interactions with subs and suppliers?
- Do you perform reviews, inspections, and have safeguards to detect/avoid counterfeit equipment, tampered HW/SW, vulnerable HW/SW and OPSEC leaks?
- Do you use the NES baseline when purchasing software?
- Do you comply with ITAR rules?
- Do you have procedures to re-create obsolescent parts?

ACCESS THE COMPLETE SCRM SELF-ASSESSMENT TOOL FOR BEST PRACTICES AND RESOURCES

SUPPLY CHAIN

A system of organizations, people, activities, information, and resources involved in moving a product or service from supplier to customer. Supply chain activities involve the transformation of natural resources, raw materials, and components into a finished product that is delivered to the end customer.

SUPPLY CHAIN RISK MANAGEMENT

A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain.

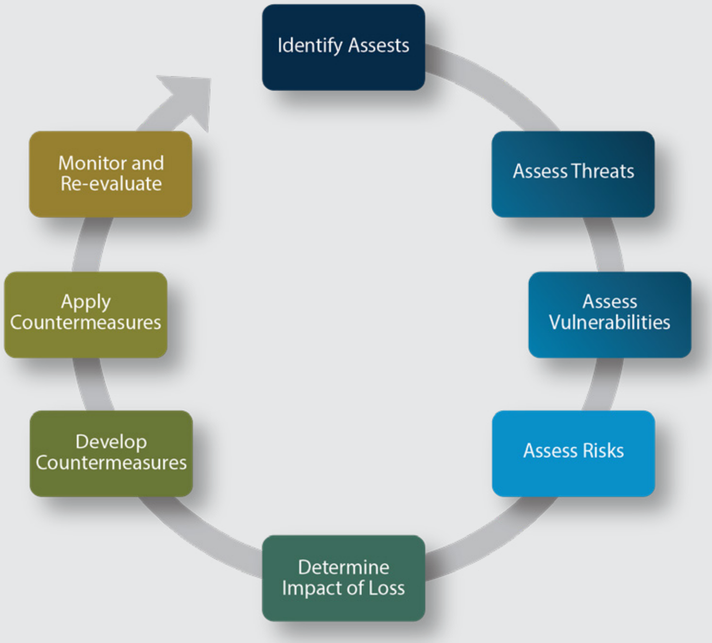
Click here for more Supply Chain Risk Management Resources.

SUPPLY CHAIN RISKS EXIST ACROSS ALL PHASE OF DEVELOPMENT

CONCEPT | DESIGN | MANUFACTURE | INTEGRATION | DEPLOYMENT | MAINTENANCE | RETIREMENT

FRAUDULANT PRODUCT	MALICIOUS INSERTION	ANTI-TAMPER	QUALITY ESCAPE	RELIABILITY FAILURE	EMERGING THREATS
Counterfeit and other than genuine and new devices from the legally authorized source including relabeled, recycled, cloned, defective, out-of-spec, etc.	The intentional insertion of malicious hard/soft coding, or defect to enable physical attacks or cause mission failure; includes logic bombs, Trojan 'kill switches' and backdoors for unauthorized control and access to logic and data.	Unauthorized extraction of sensitive intellectual property using reverse engineering, side channel scanning, runtime security analysis, embedded system security weakness, etc.	Product defect/ inadequacy introduced either through mistake or negligence during design, production, and post-production handling resulting in the introduction of deficiencies, vulnerabilities, and degraded life-cycle performance.	Mission failure in the field, due to environmental factors unique to military and aerospace environment factors such as particle strikes, device aging, hot-spots, electro-magnetic pulse, etc.	New threats, counterfeit trends, security attacks, and trust issues that combine two or more threats.

THE RISK MANAGEMENT PROCESS



SOME METHODS OF INTELLIGENCE COLLECTION INCLUDE:

- Cyber intrusions on corporate systems and/or unwitting suppliers
- Co-opted suppliers
- Traditional Insider Threat methods
- Partnerships with criminal enterprises or adoption of their methods
- Governmental control over foreign suppliers
- Development of front companies (CONUS and OCONUS)

Click here to learn more about Collection Methods and Countermeasures.

POTENTIAL COUNTERMEASURES

- Periodically change procedures
- Educate your workforce & vendors on the importance of reporting suspicious anomalies
- Develop clear and detailed incident response procedures
- Investigate suspicious anomalies
- Maintain an incident tracking repository for analysis of historical data
- Encourage supplier site visits by CI personnel for CI Awareness Training
- Conduct Self-assessments
- Consideration of CI Awareness Training requirement in contracts
- Use trusted US manufacturers, builders & installers where possible
- Diversify product selection when possible
- Continuously vet your vendors
- Stay apprised of vendor ownership changes
- Practice “need to know” with vendors
- Limit access to critical systems
- Educate yourself on how vendors protect your data on their networks
- Consistently use anti-tamper & tracking technology
- Pay close attention to shipping schedules
- Know who’s touching your materials/shipments

SUPPLY CHAIN RISK MANAGEMENT SELF ASSESSMENT

Program Name:
Program Manager Name:
Date of Assessment:
Assessor Name:

If answer is "no" to any question, review and apply the "Best Practice" highlighted from the "Key Practices and Implemetation Guide for the DoD Comprehensive National Cybersecurity Initiative 11 Supply Chain Risk Management Pilot Program"

		YES	NO	
AQUISITION				
1	Have you identified your key suppliers?			4.1
2	Do you verify company ownership? Confirm U.S. ownership?			3.2.5
3	If you use distributors, do you investigate them for potential threats?			3.2.5
4	Have you identified where additional repair parts will be purchased?			2.1
5	Are all sub-contractors and suppliers located onshore?			4.8/4.9
6	Does the program office vet suppliers for threat scenarios?			4.6/4.9
7	Do you have documents which track part numbers to manufacturers?			4.9.1
8	Can you provide a list of who you purchased your COTS software from?			4.3.2
9	Do you have an awareness regarding the likelihood of counterfeits			4.5
10	Do you safeguard key program information that may be exposed through interactions with subs and suppliers?			4.2/4.4
11	Do you perform reviews, inspections, and have safeguards to detect/avoid counterfeit equipment, tampered HW/SW, vulnerable HW/SW and OPSEC leaks?			4.6.2
12	Do you use the NES baseline when purchasing software?			4.6
13	Do you comply with ITAR rules?			4.6
14	Do you have procedures to re-create obsolescent parts?			4.7
15	Do you have procedures for securely upgrading software in the field? (Who performs the upgrades?)			4.8/NIST
16	Can you prevent from being targeted by malicious actors through the parts acquisition chain?			4.4/4.6/4.6
DESIGN/DEVELOPMENT				
17	Are you familiar with all the companies that will work on the design of the product/system?			4.2
18	Does your contractor do all engineering onshore?			3.2.5
19	Do only U.S. citizens have access to your design network?			3.2.5
20	Are you aware of who will develop your training and technical manuals?			4.5
21	If using programmable FPGA chips, do you have a plan to keep them secure?			4.8.7
22	Are you using trusted software development tools?			4.4.4
23	Are you using trusted information assurance controls to safeguard technical data in the development environment (networks, PC's test equipment and configuration systems)?			4.1.3/IA
24	Do you know how to evaluate open source software?			4.4/4.7
25	Are your software compilers controlled for authorized access only?			4.6.4
26	Do you know how your contractor will test and configure software code?			4.6.6

LOGISTICS				
27	Does your program have documented configuration management, tracking and version controls in place?			4.3/4.9.4
28	Have you thought about what events (environmental or man-made)can interrupt your supply chain?			4.8.6
29	Are your completed parts controlled, so they are never left unattended or exposed to tampering?			4.2.8
30	Are completed parts locked up?			4.2.6
31	Do you have a process that insures integrity when ordering inventory?			4.2.7
32	Do you periodically inspect your inventory for exposure or tampering?			4.3.3
33	Are upgrades to your IT infrastructure evaluated for possible tampering?			4.3.4
34	Do you have secure material destruction procedures for unused and scrap parts?			4.10.7
35	Is there a documented chain of custody for the deployment of products and systems?			4.3.4
POLICY/PROCEDURES				
36	Do you have definitive policies and procedures that help minimize supply chain risk?			4.3/4.1.3
37	Do you define and manage system criticality and capability?			3.2.5
38	Does everyone associated with the program (program managers, prime contractors, subcontractors, etc.) understand the threats and risks in the program's supply chain?			3.2.6
39	Are all support contractors US citizens?			4.8.2
40	Do you have "insider threat" controls in place?			SC
41	Are you familiar enough with everyone that touches your product or system to know if they pose a threat?			Rev 1
42	Do you use any protective technologies?			4.6.1/4.8.6
43	Do you enter data into the GIDEP database?			GIDEP
44	Do you use, record, and track risk mitigation options throughout the life cycle of the product or system?			4.5/3.2.1
45	Do you have counterintelligence meetings?			Rev 1
46	Have all of your contractors signed non-disclosure agreements?			SF 312
47	Is there foreign national access to your unclassified network?			FOCI
48	Do you make your supply chain risk management policies/procedures a requirement for suppliers?			4.4.1
49	Do your supply chain risk management policies/procedures take into account secondary sourcing?			4.4.1
50	Do you develop and use a Risk Management plan?			RMP
51	Do you have a Risk Management Review Board			DAU
52	Does anyone have access to your data from an external connection?			4.9.1
53	For contractors who use your data on their system, do they have adequate security controls to protect the data?			4.2/4.2.1

TEN PRACTICES, IMPLEMENTED IN THEIR ENTIRETY, COVER THE COMPLETE SOFTWARE DEVELOPMENT LIFECYCLE.

4.1	Uniquely Identify Supply Chain Elements, Processes, and Actors
4.2	Limit Access and Exposure within the Supply Chain
4.3	Establish and Maintain the Provenance of Elements, Processes, Tools, and Data
4.4	Share Information within Strict Limits
4.5	Perform SCRM Awareness and Training
4.6	Use Defensive Design for Systems, Elements, and Processes
4.7	Perform Continuous Integrator Review
4.8	Strengthen Delivery Mechanisms
4.9	Assure Sustainment Activities and Processes
4.1	Manage Disposal and Final Disposition Activities throughout the System or Element Life Cycle

2.1 (Paragraphs 6-8)

Today's multifaceted global economy and manufacturing practices make corporate ownership and control more ambiguous when assessing supply chain vulnerabilities. For example, foreign-based companies sometimes manufacture and assemble products and components in the United States, and U.S.-based companies sometimes manufacture products and components overseas, or domestically employ foreign workers.

Though globalization and its consequences are permanent and likely to have a greater impact over time, this growing complexity reduces both the depth and breadth of visibility and traceability achievable by the federal acquirer. This lack of visibility and traceability increases the acquirer's risk of being unable to manage the risks associated with intentional and unintentional compromises which may be introduced through a variety of means, including counterfeit materials or malicious software.

Currently, federal departments and agencies as well as private sector integrators and suppliers use widely varied ICT SCRM practices. This fact is underscored by the report from the University of Maryland's Supply Chain Management Center, which indicates that there is an overall lack of emphasis on ICT SCRM from companies of all sizes (see Appendix D). As a result, the potential for intentional and unintentional compromise of federal information systems increases.

<<BACK TO TABLE

3.2.1 Determine Risk

Mission/business owners, information system security personnel, stakeholder representatives, and possibly outside experts should conduct applicable risk analyses and identify applicable supply chain risk mitigations. Acquirers can use existing methodologies such as NIST SP 800-30 Revision 1 to conduct the assessment. <<BACK TO TABLE

3.2.5 Complete Procurement

SOW/SOO

The mission/business owner or designee should develop a SOW/SOO that includes a detailed description of the specific functional, technical, quality, and security requirements and qualifications. This document should include the selected ICT SCRM practices (general and technical requirements, and verification and validation activities) and NIST SP 800-53 controls relevant to an integrator and, in some instances, a supplier supporting acquirer activities. Requirements developed for market analysis and any adjustments made from the results of the RFI process should provide significant input to the RFP or RFQ.

The following should be considered when developing the SOW/SOO requirements:

- Appropriate level of risk distribution among the acquirer, integrator, and suppliers;
- Integrator's level of responsibility for supplying assurance for systems and elements;
- Criticality analysis including:
  10 Effective July 1, 2009, the FAR requires federal agencies to post all contractor performance evaluations in the Past Performance Information Retrieval System (PPIRS) http://www.ppirs.gov/.
  NIST IR 7622, Notional Supply Chain Risk Management Practices for Federal Information Systems

22

- Determining from a mission criticality analysis, which system elements are critical. A system decomposition is required to identify which elements are critical for mission criticality;
- A dependency analysis to determine if any noncritical elements have a mission-critical impact on the critical elements. This will ascertain if mitigation (technology or process) is required to protect the critical components and in turn the mission; and
- Determining the appropriate level of access to the critical elements for the protection of these elements and the mission they support;
- Requirements for processes (including test and evaluation [T&E] processes) and inclusion of these processes in contract documents;
- The methodology used by integrators to select/manage their suppliers and whether the integrator or supplier imposes similar requirements on their downstream suppliers;
- Requirements for respondents to demonstrate that they have the necessary security measures in place to manage ICT supply chain risks (e.g., attestation, provision of third-party certifications, etc.); and
- How acquirer's and integrator's or supplier's proprietary data will be used, how long it will be kept, with whom it can be shared, and what intellectual property protections will prevail. <<BACK TO TABLE

3.2.5 Evaluation Criteria

ICT SCRM-focused evaluation criteria can be applied to both integrators and suppliers and can be integrated into the overall evaluation criteria for individual acquisitions.

Identifying and gathering information on the integrator or supplier organization is critical to managing supply chain risk. Examples of such information include:

- Organizational History – years of operation, Central Contractor Registry (CCR) registration record

- Foreign Interests and Influences (including ownership)
- Financial History and Status – Size of Organization, credit rating (including Dun and Bradstreet [DUNS] record)
- Facilities – location, history of physical security violations, facilities management policies
- Policies for Personnel Security Review and Control
- Integrator's ability to pass ICT SCRM requirements past first tier suppliers. <<BACK TO TABLE

3.2.5 Acquisition-Specific Risk Assessment

A risk assessment should be conducted as part of the RFP/RFQ review. The criteria for this assessment should be defined using mission, functional, quality, and security requirements. Acquirers can use existing methodologies such as NIST SP 800-30 Revision 1 to conduct the assessment. Data to support this assessment should be collected from a variety of sources, such as:

- Integrator or supplier security track record (e.g., compilation of publicly available financial, operational, legal, and technical information);
- Software security training and awareness within the integrator or supplier organization;
- Security monitoring both of the element and element processes;
- Timeliness of vulnerability mitigation of element and element processes;
- Policies for service confidentiality;
- Policies for information sharing and access control;
- Policies for integrator or supplier information security;
- Results of independent third-party evaluations; and
- Security certifications.

Federal department and agency acquirers may consult with their counterparts in other agencies who are using the product being acquired to obtain information to support this assessment. Other items may be added to the evaluation as appropriate. <<BACK TO TABLE

3.2.5 Element's security track record

Elements are subject to both intentional and unintentional insertion of malicious functionality, weaknesses, and counterfeits. Some key items addressed as part of the element evaluation should include:

- Architecture/Design characteristics – including built-in defenses and whether they meet functional requirements.
- Element history and licensing – reviewing element

NIST IR 7622, Notional Supply Chain Risk Management Practices for Federal Information Systems

21

quality, reliability, security incidents, licensing terms, indemnifications, etc.

- Publicly available record of vulnerabilities (e.g., using the National Vulnerability Database) associated with the element and the process for addressing incidents, root cause analyses, and fixes. <<BACK TO TABLE

32.5x

32.5x The mission/business owner or designee should develop a SOW/SOO that includes a detailed description of the specific functional, technical, quality, and security requirements and qualifications. This document should include the selected ICT SCRM practices (general and technical requirements, and verification and validation activities) and NIST SP 800-53 controls relevant to an integrator and, in some instances, a supplier supporting acquirer activities. Requirements developed for market analysis and any adjustments made from the results of the RFI process should provide significant input to the RFP or RFQ. <<BACK TO TABLE

3.2.6 Operational Contract Execution

Once a system becomes operational, the operating environment may change. Changes include, but are not limited to, suppliers, elements, delivery processes, and business processes. These changes may alter, add, or reduce ICT supply chain risks. During operations, acquirers should continue to perform ICT SCRM, including the assessment of foundational enterprise practices. The acquirer will need to ensure that the integrator or supplier understands supply chain risk and provides information on applicable changes to the element, environment, vulnerabilities, and patches on an ongoing basis. The following activities will help the acquirer maintain supply chain oversight and improve processes for future procurements:

- Collect, analyze, record, and disseminate ICT SCRM lessons learned within the project and within the larger organization(s). This information will help enhance immediate project performance and provide input into the enterprise ICT SCRM process;
- Collect information on whether the trade-offs that were made during the procurement with regards to mitigating ICT supply chain risks substantially increased that risk;
- Identify gaps that were not addressed in past projects and how they can be filled;
- Monitor and periodically (or continuously if appropriate) reevaluate changes in the risk environment that impact the supply chain including technology innovation, operational environment, regulatory environment, etc. Respond to change where appropriate through modifying ICT SCRM requirements or if needed, modifying relationships with integrators or suppliers. Note: (1) Use information as available, including information from commercial sources, U.S. government agencies, and intelligence information as appropriate. (2) Respond to such changes when appropriate, e.g., by adding additional

countermeasures (such as additional practices from this document) or changing to a less risky integrator or supplier;

- Integrate ICT SCRM considerations in continuous monitoring activities; and
- Collect feedback on integrator or supplier responsiveness and effectiveness at mitigating risks per acquirer requests.

The acquirer should use the practices in Section 4 to address supply chain assurance when acquiring replacement components or field additions/modifications/upgrades, particularly if they do not go through traditional acquisition processes that examine ICT supply chain risks.
Acquirers and integrators need to be aware of the time frame within which their elements and systems are expected to become obsolete and plan for replacing and upgrading these elements and systems. Systems that have a long life cycle may require a substantial number of elements that are no longer available from the original component manufacturer or through their franchised distributors. In some cases, upgrades may not be compatible with the system (backwards compatible) or supported by the original manufac <<BACK TO TABLE

4.1 Uniquely Identify Supply Chain Elements, Processes, and Actors

Knowing who and what is in an enterprise's supply chain is critical to gain visibility into what is happening within it, as well as monitoring and identifying high-risk events and activities. Without reasonable visibility and traceability into supply chain, e.g., elements, processes, and actors, it is impossible to understand and therefore manage risk, and to reduce the likelihood of an adverse event. Uniquely identifying organizations, personnel, mission and element processes, communications/delivery paths and elements, as well as the components and tools used, establishes a foundational identity structure for assessment of ICT supply chain activities. For example, labeling (e.g., serial number) and tagging (e.g., radio-frequency identification [RFID] tag) software packages and modules, hardware devices, individual elements, and processes that surround them can be used for this purpose. <<BACK TO TABLE

4.1.3 Suppliers -– General Requirements

a) Apply unique identification requirements to delivered elements (e.g., serial numbers, date codes, license labels, etc.).
b) Ensure that identification methods are sufficient to support provenance in the event of a supply chain issue or adverse supply chain event.
c) Establish policies and procedures that require identification methods to support provenance in the event of a supply chain issue or adverse supply chain event.
d) Define, design, and implement roles that limit privilege and create redundancy throughout the element life cycle to mitigate the risk of a single role being able to, intentionally or unintentionally, create adverse consequences.
e) Require protection and safeguarding of authentication mechanisms. <<BACK TO TABLE

4.2 Limit Access and Exposure within the Supply Chain

Elements that traverse the supply chain are subject to access by a variety of actors. It is critical to limit such access to only as much as necessary for those actors to perform their role(s) and to monitor that access for supply chain impact. Access control techniques exist that may be useful in providing needed granularity to ensure that only appropriate actors can monitor or change supply chain elements, element processes, organizations, organizational processes, information, communications, and systems covering the comprehensive supply chain. <<BACK TO TABLE

4.2.1

a) Establish an internal policy for the broad responsibilities of assigning access control to information, systems, supply chain elements, element processes, as well as key personnel and organizational activities as deemed necessary to protect the confidentiality, integrity, and availability of supply chain elements and processes throughout the system/element life cycle. <<BACK TO TABLE

4.2.1 Acquirer - Programmatic Activities

h) Establish an internal policy for remote access, including allowing access to the organization's location and third-party locations, media, network, and other items to be determined.
i) Establish and document a policy describing allowed methods of remote access to elements, systems, processes, and organizations. <<BACK TO TABLE

4.2.1 Acquirer - Programmatic Activities

a) Establish an internal policy for the broad responsibilities of assigning access control to information, systems, supply chain elements, element processes, as well as key personnel and organizational activities as deemed necessary to protect the confidentiality, integrity, and availability of supply chain elements and processes throughout the system/element life cycle.

c) Identify the individuals (roles) and organizations with responsibility for the design, development, and implementation of access controls, to include use of information security, operations security, physical security, industrial security, and IA tactics, techniques, procedures, and tools.

j) Establish and enforce requirements for personnel security reviews and assessments for acquirer personnel. These reviews and assessments should include personnel who have exposure or access to sensitive information, such as elements, element processes, business activities, or integrator or supplier intellectual property. Special attention should be paid to those personnel with the technical knowledge or understanding of enterprise processes that would allow them to obtain unauthorized exposure of, or access to, elements or processes that could result in compromise or loss. <<BACK TO TABLE

4.2.4 Integrator – Technical Implementation Requirements

a) Develop and implement roles throughout the system life cycle to limit opportunities and means available to individuals performing these roles to expose elements, processes, systems, or information, including requirements to potential compromise.
b) Employ automated and repeatable mechanisms, when feasible, to facilitate monitoring and controlling: a. Various access methods (physical and logical); b. Access occurring with no manual observers and controllers; and c. High volume of access requested in a given short period of time or simultaneously.
c) Employ automated and repeatable mechanisms, when feasible, to facilitate the maintenance and review of access records.
d) Maintain records of all physical and logical accesses and activities, both authorized and unauthorized, including by visitors and regular individuals in accordance with existing acquirer and integrator polices.
e) Provide access control protection for both remote and mobile devices and the use of remote and mobile access points to the supply chain infrastructure.
f) Obtain chain-of-custody evidence and require tamper-evident packaging for critical hardware elements.
g) If two or more unique identities have access to an element, process, organization, information, or system, use multifactor authentication mechanisms. Two or more unique identities can include one user and one administrator when feasible.
h) Limit the use of a unique identity for multiple uses by restricting privileges and permissions (e.g., with implementation of single sign-on Personal Identity Verification). **<<BACK TO TABLE**

4.2.6 Acquirer - Verification and Validation Activities

a) Assess security risks to physical and logical access controls intended to prevent unauthorized exposure of, or access to, tools, processes, people, and systems in the supply chain that create supply chain elements or information about such elements or unauthorized introduction of counterfeit parts.
b) Perform security checks at the physical and logical boundary of the element, element processes, facilities, and system, for unauthorized access to or export of information, elements, tools, and materiel used in element processes.
c) Prevent, detect, and document any physical tampering or altering of access control mechanisms.
d) Review the integrator's processes and procedures aimed at limiting exposure of system and elements uses. **<<BACK TO TABLE**

4.2.7 Integrator - Verification and Validation Requirements

a) Demonstrate that a mix of personnel, physical, and logical access controls are implemented which provide a level of protection commensurate with the sensitivity/criticality of the services provided or the elements procured.
b) Perform technical and procedural audits of mechanisms used to shield information related to elements, including uses, requirements, and metadata.
c) Employ Red Team approaches to identify potential pathways or opportunities for adversaries to exploit deficits or weaknesses in supply chain processes that would result in the exposure of the element or associated information including uses of element.
d) Assess the effectiveness of alternative configurations in protecting access of elements, processes, systems, and information for the purposes of confidentiality, integrity, and availability.
e) Test internal access controls for the ability to detect anomalous behavior and facilitate timely intervention to prevent or reduce adverse consequences.

<<BACK TO TABLE

4.2.8 Supplier – Verification and Validation Requirements

a) Demonstrate use of access control mechanisms across the system or element life cycle and the associated supply chain.
b) Demonstrate ability to intervene in a timely manner to prevent or reduce adverse consequences within the supply chain. **<<BACK TO TABLE**

4.3 Establish and Maintain the Provenance of Elements, Processes, Tools, and Data

Provenance can be achieved through both physical and logical techniques, such as Configuration Management (CM) for tracking changes to the elements and documenting the individuals who approved and executed these changes; robust identity management and access control to establish and record authorized or unauthorized activities or behaviors; and identification/tagging of elements, processes, roles, organizations, data, and tools. **<<BACK TO TABLE**

4.3 Establish and Maintain the Provenance of Elements, Processes, Tools, and Data

All system elements originate somewhere and may be changed throughout their existence. The record of element origin along with the history of, the changes to, and the record of who made those changes is called "provenance." Acquirers, integrators, and suppliers should maintain the provenance of elements under their control to understand where the elements have been, the change history, and who might have had an opportunity to change them.
Provenance is used when ascertaining the source of goods such as computer hardware to assess if they are genuine or counterfeit. Provenance allows for all changes from the baselines of components, component processes, information, systems, organizations, and organizational processes, to be reported to specific actors, functions, locales, or activities. Additionally, creating and maintaining provenance within the supply chain helps achieve greater traceability in case of an adverse event and is critical for understanding and mitigating risks. Doing so requires a process by which changes to objects and activities within a supply chain and the persons, organizations, or processes responsible for authorizing and performing such changes are inventoried, monitored, recorded, and reported.
Provenance can be achieved through both physical and logical techniques, such as Configuration Management (CM) for tracking changes to the elements and documenting the individuals who approved and executed these changes; robust identity management and access control to establish and record authorized or

unauthorized activities or behaviors; and identification/tagging of elements, processes, roles, organizations, data, and tools. <<BACK TO TABLE

4.3.2 Integrators – General Requirements

l) Establish and implement a process for the CM of documentation, COTS or GOTS elements, and custom systems/elements. Perform security assessments of the CM processes and systems to attempt the detection of ongoing attacks (including the CM systems). <<BACK TO TABLE

4.3.3 Suppliers – General Requirements

a) Provide evidence of formal processes for documenting roles, responsibilities, and procedures to include the management information and documentation for establishing provenance.
b) Provide evidence on element baselines and maintenance throughout the system or element life cycle, including as part of logistics. Establish and implement a policy to monitor and maintain a valid baseline.
c) Identify and implement appropriate levels of confidentiality, integrity, and availability including spare parts and warehoused systems/elements.
d) Ensure that the provenance of supply chain configuration items (e.g., in the CM system) is protected from unauthorized access and change.
e) Upon request, make available up-to-date product histories that document element changes including retired elements under warranty. <<BACK TO TABLE

4.3.4 Integrators – Technical Implementation Requirements

a) Employ the use of mechanisms (tools and techniques) to assist in developing and maintaining the provenance of tools, data, and processes used throughout the system or element life cycle, including but not limited to use of CM or Configuration Control systems.
b) Design and implement a two-person rule for system/element/process and configuration changes, where change in an element or process cannot be reversed, or where non-repudiation of change is not possible. Identify, document, and review any exceptions from the mandatory configuration settings for individual elements, systems, and processes based on the development, operational, and delivery requirements.
c) Employ automated mechanisms, both centrally and through a trusted distributed CM system, whereby configuration settings are applied, managed, and verified. (Note: Most automated CM systems work in both a central and distributed manner and can be set up to have a trusted distributed CM environment.)
d) Incorporate detection mechanisms for unauthorized, security-relevant configuration changes into the integrators' incident response capability to ensure that detected CM events associated with element changes are tracked, monitored, corrected, and available for historical purposes.
e) Ensure that backup information systems containing CM information implement immutable chains (e.g., digital signatures proving a sequence of events) and deploy a recovery process when a CM information system is breached or unavailable.
f) Implement accountability for all changes in configuration items by recording the identity of each individual who is making a change, when each change was made, and exactly what the change was. This information should be authenticated such that it cannot be repudiated (Digital signatures can be used to confirm this information.).
g) Document the process for ensuring traceability when moving information, elements, and processes across physical and logical boundaries including any approvals required. This may include the identification of key personnel for the handling of information.
h) Establish performance and sub-element baselines for the system and system elements. This helps to detect unauthorized tampering/modification during repairs/refurbishing by comparing the state of the returned element with the original state per element baseline.
i) Maintain chain of custody for any hardware element sent to an external provider for repair <<BACK TO TABLE

4.4.1 Acquirer - Programmatic Activities

q) Diversify/disperse how the product is acquired in order to make it difficult for an adversary to determine how, when, and where an element will be acquired.
<<BACK TO TABLE

4.4.1 Acquirer - Programmatic Activities

a) Establish a policy about the sharing of information throughout the life cycle of the systems/elements. Include the following topics:
a. Which information is to be shared and which information is to be withheld from sharing;
b. Those individuals and organizations eligible to receive, store, use, and retransmit information;
c. The duration of information-sharing activities, as well as the events on which information sharing will begin and will be terminated;
d. Standards and requirements for protection of data at rest and in motion;
e. Standards to be used to protect shared information against unauthorized disclosure, access, modification, dissemination, or destruction, and unauthorized use of data and information;
f. Requirements for establishing identity of participants in information-sharing arrangements;
g. The means by which information sharing is executed and the mechanisms used to provide protection of information commensurate with the importance of such information; and
h. The planning and execution of audits of information-sharing activities. <<BACK TO TABLE

4.4.1

e) Protect requirements and supporting documentation, including acquirer, integrator, and supplier intellectual property, from exposure or access that could result in the compromise or loss the confidentiality, integrity, or availability of the requirements. <<BACK TO TABLE

4.4.1 Acquirer - Programmatic Activities

g) Develop approaches that encourage integrators to gain visibility into their supply chains as deeply as possible and are reasonable. (1) Develop incentives that reward integrators for providing program-specific detailed technical information and technical data on products and services throughout the life cycle; and (2) include requirements that address the selection of open source elements. <<BACK TO TABLE

j) Encourage integrators to evaluate, document, and share element/element process information (including open source) that could result in weaknesses or vulnerabilities and if exploited, could result in loss or compromise.

4.4.1 Acquirer - Programmatic Activities

a) Establish a policy about the sharing of information throughout the life cycle of the systems/elements. Include the following topics:

q) Diversify/disperse how the product is acquired in order to make it difficult for an adversary to determine how, when, and where an element will be acquired. When appropriate, make the supply route less predictable through dynamic sourcing from multiple suppliers. <<BACK TO TABLE

4.4.4 Integrators - Technical Implementation Requirements

d) Apply identity management, access controls, and CM to the requirements process to ensure the confidentiality, integrity, and availability of requirements as well as supporting data, information, and requirements development tools. <<BACK TO TABLE

4.5 Perform Supply Chain Risk Management Awareness and Training

A strong supply chain risk mitigation strategy cannot be put in place without significant attention given to training federal department and agency acquirer personnel and integrator personnel on supply chain policy, procedures, and applicable management, operational, and technical controls and practices. NIST SP 800-50, Building an Information Technology Security Awareness and Training Program, provides guidelines for establishing and maintaining a comprehensive awareness and training program. Additionally, the ISO/IEC 27001 information security management standard and the ISO 28000:2007 supply chain process integration and certification standard provide information on developing an organization-wide program that includes training. This practice focuses on supply chain-specific awareness and training practices. In general, the training should include all applicable practices found in this document. <<BACK TO TABLE

4.6.1 Acquirer – Programmatic Activities

a) Define, design, and implement roles for individuals, organizations, elements, and element processes throughout the system or element life cycle to limit or constrain:
1. Unmonitored or uncontrolled activity across multiple elements, processes, organizations, or systems;
2. The opportunities or means for unauthorized exposure that can lead to the compromise of elements, element processes, systems, or information; and
3. The inability to detect or monitor adverse events.
b) Define and document acquisition processes by which elements are selected for use in systems and integrate these into the organization's operational practices, acquisition strategies, and procurement activities. Specify use of genuine and tested elements. If such elements are not available, require a vetting process for use of secondary market elements.
c) Use available information about applicable <<BACK TO TABLE

4.6.1 Acquirer – Programmatic Activities

f) Establish organizational procedures that require design processes to address protective or corrective options which either avoid mission interruption or permit graceful degradation of the system should the system be attacked or compromised. <<BACK TO TABLE

4.6.2 Integrators - General Requirements

s) Perform manual review of elements, processes, and system(s) to identify and remediate any weaknesses and vulnerabilities including peer reviews (e.g., walk-throughs and inspections) and comprehensive or sampled reviews. Employ independent internal or external reviewers. <<BACK TO TABLE

4.6.3 Suppliers – General Requirements

d) If available, provide assessment results of potential failure modes and effects on various proposed element designs based on the application of observed adversary tactics, techniques, procedures, and tools. <<BACK TO TABLE

4.6.4 Integrators – Technical Implementation Requirements

a) Use existing resources such as market/technical analysis results, prequalified product lists (e.g., available from General Services Administration [GSA], DHS, or internal integrator list) for identifying candidate elements. If applicable, require elements to have certifications and validations such as Common Criteria, FIPS 140-2 validation, and Federal Desktop Core Configuration (FDCC)/ United States Government Configuration Baseline (USGCB). <<BACK TO TABLE

4.6.4 Integrators – Technical Implementation Requirements

y) Prepare personnel participating in manual reviews by reporting or demonstrating known adversary tactics, techniques, procedures, and tools for exploiting weaknesses or deficits in systems/elements, assemblies, information systems, or processes. <<BACK TO TABLE

4.6.6 Acquirer – Verification and Validation Activities

a) Review integrators' quality assurance processes to ensure compliance with requirements, federal procurement policy, and FAR.
b) Examine the element to ensure that it is as specified in requirements and that it is new, genuine, tested, and that all associated licenses (including support agreements) are valid. <<BACK TO TABLE

4.7 Perform Continuous Integrator Review

Continuous integrator review is an essential practice used to ascertain that defensive measures have been deployed. It includes testing, monitoring, auditing, assessments, and any other means by which the acquirer observes integrator practices. The purpose of continuous integrator review is to validate compliance with requirements, ascertain that the system behaves in a predictable manner under stress, and detect and classify weaknesses and vulnerabilities of elements, processes, systems, and any associated metadata. <<BACK TO TABLE

4.7.1

h. Define criteria and thresholds for identifying and tracking critical elements that require modification or replacement throughout the supply chain. These thresholds should be set well before an element's expected retirement from service and based, for example, on mean-time-between-failures (MTBF) for hardware and the number of releases for software. <<BACK TO TABLE

4.7.1 Acquirer – Programmatic Activities

p) When practical for evaluating potential critical system elements, prefer integrators and suppliers that have incorporated static and dynamic analysis as best practices into their system or element life cycle process before: 1) making a make-buy decision; 2) selecting COTS, GOTS, custom, or open source elements; and 3) accepting COTS, GOTS, custom, or open source elements into the system. <<BACK TO TABLE

4.8.2 Integrators – General Requirements

a) Establish processes to assure that the system or element will be delivered when needed:
a. Modify the delivery path so that it is difficult to prevent delivery (e.g., via sabotage); and
b. Define multiple vetted delivery paths, in case a delivery path is unavailable or compromised.
b) Establish minimum baselines for supply chain delivery, processes, and mechanisms.
c) Where appropriate, use trusted contacts and ship via a protected carrier (such as U.S. registered mail, using cleared/official couriers, or a diplomatic pouch). Protect the system and element while storing before use (including spares).
d) Design delivery mechanisms to avoid exposure or access to the system and element delivery processes, and use of the element during the delivery process.
e) Implement delivery processes for the intended logical and physical transfer and receipt of elements to be done by authorized personnel.
f) Ensure education and training for personnel inventory management policies and processes.
g) Use nondestructive techniques or mechanisms to determine if there is any unauthorized access throughout the physical delivery process.
h) Maintain a level of physical and/or logical access control (i.e., locking file cabinets on the integrator premises), where relevant, for all purchase order/delivery authorizations for physical product delivery. <<BACK TO TABLE

4.8.2 Integrators – General Requirements

a) Establish processes to assure that the system or element will be delivered when needed:
    a. Modify the delivery path so that it is difficult to prevent delivery (e.g., via sabotage); and
    b. Define multiple vetted delivery paths, in case a delivery path is unavailable or compromised. <<BACK TO TABLE

4.8.4 Integrators - Technical Implementation Requirements

Stipulate assurance levels and monitor logical delivery of products and services, requiring downloading from approved, verification-enhanced sites. Consider encrypting elements (software, software patches, etc.) at rest and in motion throughout delivery. Mechanisms that use cryptographic algorithms must be compliant with NIST FIPS 140-2. <<BACK TO TABLE

4.8.6 Acquirer - Verification and Validation Activities

a) Verify that the integrator has documented processes for the hardening of delivery mechanisms when required, including use of protective physical and logical packaging approaches for systems, elements, and associated technical or business process information, and protection of element processes throughout the system and element life cycle. <<BACK TO TABLE

4.8.6 Acquirer - Verification and Validation Activities

d) Verify that the integrator has realistic continuity plans to ensure that systems and elements will be available even in a stressed/emergency environment.
<<BACK TO TABLE

4.8.7 Integrators - Verification and Validation Requirements

b) Perform physical and information security reviews of supply chain mechanisms used by suppliers to assess the effectiveness of measures intended to reduce opportunities for exposure of, or access to, elements, processes, or information regarding elements or processes. <<BACK TO TABLE

4.9.1 Acquirer – Programmatic Activities

a) Include procurement clauses in formal service and maintenance agreements that reduce supply chain risk.
b) When acquiring OEM elements, including refurbished elements, establish a contractual relationship with the originator or original manufacturer that provides vetted, competent support where possible <<BACK TO TABLE

4.9.1 Acquirer - Program Activities

s) Require establishment of a process for managing supply chain vulnerabilities, including detecting, tracking/logging, selecting a response, performing the response, and documenting the response. This provides a feedback loop for continuous improvement of supply chain elements and element processes and corrective action handling for any vulnerability or other issues that require addressing. Similarly, a standardized due process procedure may be needed to ensure that integrators, suppliers, element and sub-suppliers have the opportunity to address and/or appeal any actions that acquirers may seek to impose.
<<BACK TO TABLE

4.9.2 Integrators – General Requirements

a) Avoid introducing new actors in maintenance activities where possible (e.g., keep original manufacturers and/or OEM-authorized suppliers). If new actors need to be added, implement a vetting process for them. Notify the acquirer of any major changes in a maintenance organization's structure or process (e.g.physical move to a different location, change in ownership, outsourcing, and/or changes in personnel). <<BACK TO TABLE

4.9.4 Integrators -– Technical Implementation Requirements

b) Protect system elements from tampering by using a variety of methods. Methods can include robust configuration management, limited privileges, checking cryptographic hashes, and applying anti-tamper techniques. Use existing vulnerability and incident management capabilities to identify potential supply chain vulnerabilities. This provides a feedback loop for continuous improvement of supply chain elements and element processes. <<BACK TO TABLE

4.10.7 Integrators - Verification and Validation Requirements

a) Ensure the adequacy of the destruction method for controlled items (e.g., NIST 800-80 controls for removable media).
b) Verify suppliers' security procedures to govern the transfer of elements and acquirer's sensitive information.
c) Ensure that items subject to controlled disposal are accurately identified, marked, and recorded for traceability <<BACK TO TABLE

Information Assurance (IA)

Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.
CNSSI No. 4009 <<BACK TO TABLE

NIST SP 800-34; CNSSI-4009 System Development Life Cycle (SDLC)

The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation. <<BACK TO TABLE

Revision 1

Revision 1 to conduct the assessment. Data to support this assessment should be collected from a variety of sources, such as:

- Integrator or supplier security track record (e.g., compilation of publicly available financial, operational, legal, and technical information);
- Software security training and awareness within the integrator or supplier organization;
- Security monitoring both of the element and element processes;
- Timeliness of vulnerability mitigation of element and element processes;
- Policies for service confidentiality;
- Policies for information sharing and access control;
- Policies for integrator or supplier information security;
- Results of independent third-party evaluations; and

- Security certifications.

Senior Information Security Officer (SISO) - The Senior Information Security Officer, also known as SISO, is responsible for promulgating policies on security integration in the SDLC and the development and implementation of security policy, guidelines, and procedures pertaining to SCRM. The SISO plays a leading role in introducing an appropriately structured methodology to help identify, evaluate, and minimize supply chain risks to the organization. In addition, the SISO is responsible for analyzing and developing:

- Procedures for performing, analyzing, and utilizing integrator or supplier assessments; and
- Technical mitigation strategies derived from the integrator or supplier assessments, ensuring that assessments are performed by a third party (not necessarily an external party).

<<BACK TO TABLE

Revision 1

Revision 1 to conduct the assessment. Data to support this assessment should be collected from a variety of sources, such as:

- Integrator or supplier security track record (e.g., compilation of publicly available financial, operational, legal, and technical information);
- Software security training and awareness within the integrator or supplier organization;
- Security monitoring both of the element and element processes;
- Timeliness of vulnerability mitigation of element and element processes;
- Policies for service confidentiality;
- Policies for information sharing and access control;
- Policies for integrator or supplier information security;
- Results of independent third-party evaluations; and
- Security certifications.

<<BACK TO TABLE

SC

Many of the practices in this document are based on good security practices and procedures found in NIST Special Publications (SPs) like NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations; the National Defense University, Software Assurance in Acquisition: Mitigating Risks to the Enterprise; and the National Defense Industrial Association (NDIA), Engineering for System Assurance, and then expanded upon to include supply chain-specific implications. Additional guidance that may have supply chain implications includes, but is not limited to, International Traffic in Arms Regulations (ITAR) and Customs-Trade Partnership Against Terrorism (CTPAT).

<<BACK TO TABLE