3.20 SUPPLY CHAIN RISK MANAGEMENT

Quick link to Supply Chain Risk Management Summary Table

SR-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] supply chain risk management policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and

c. Review and update the current supply chain risk management:

   1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Supply chain risk management policy and procedures address the controls in the SR family as well as supply chain-related controls in other families that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of supply chain risk management policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to supply chain risk management policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PM-30, PS-8, SI-12.

Control Enhancements: None.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

References: [FASC18], [41 CFR 201], [EO 13873], [CNSSD 505], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-100], [SP 800-161].

SR-2 SUPPLY CHAIN RISK MANAGEMENT PLAN

Control:

a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: [*Assignment: organization-defined systems, system components, or system services*];

b. Review and update the supply chain risk management plan [*Assignment: organization-defined frequency*] or as required, to address threat, organizational or environmental changes; and

c. Protect the supply chain risk management plan from unauthorized disclosure and modification.

Discussion: The dependence on products, systems, and services from external providers, as well as the nature of the relationships with those providers, present an increasing level of risk to an organization. Threat actions that may increase security or privacy risks include unauthorized production, the insertion or use of counterfeits, tampering, theft, insertion of malicious software and hardware, and poor manufacturing and development practices in the supply chain. Supply chain risks can be endemic or systemic within a system element or component, a system, an organization, a sector, or the Nation. Managing supply chain risk is a complex, multifaceted undertaking that requires a coordinated effort across an organization to build trust relationships and communicate with internal and external stakeholders. Supply chain risk management (SCRM) activities include identifying and assessing risks, determining appropriate risk response actions, developing SCRM plans to document response actions, and monitoring performance against plans. The SCRM plan (at the system-level) is implementation specific, providing policy implementation, requirements, constraints and implications. It can either be stand-alone, or incorporated into system security and privacy plans. The SCRM plan addresses managing, implementation, and monitoring of SCRM controls and the development/sustainment of systems across the SDLC to support mission and business functions.

Because supply chains can differ significantly across and within organizations, SCRM plans are tailored to the individual program, organizational, and operational contexts. Tailored SCRM plans provide the basis for determining whether a technology, service, system component, or system is fit for purpose, and as such, the controls need to be tailored accordingly. Tailored SCRM plans help organizations focus their resources on the most critical mission and business functions based on mission and business requirements and their risk environment. Supply chain risk management plans include an expression of the supply chain risk tolerance for the organization, acceptable supply chain risk mitigation strategies or controls, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the plan, a description of and justification for supply chain risk mitigation measures taken, and associated roles and responsibilities. Finally, supply chain risk management plans address requirements for developing trustworthy, secure, privacy-protective, and resilient system components and systems, including the application of the security design principles implemented as part of life cycle-based systems security engineering processes (see SA-8).

Related Controls: CA-2, CP-4, IR-4, MA-2, MA-6, PE-16, PL-2, PM-9, PM-30, RA-3, RA-7, SA-8, SI-4.

Control Enhancements:

(1) SUPPLY CHAIN RISK MANAGEMENT PLAN | ESTABLISH SCRM TEAM

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

Establish a supply chain risk management team consisting of [*Assignment: organization-defined personnel, roles, and responsibilities*] to lead and support the following SCRM activities: [*Assignment: organization-defined supply chain risk management activities*].

Discussion: To implement supply chain risk management plans, organizations establish a coordinated, team-based approach to identify and assess supply chain risks and manage these risks by using programmatic and technical mitigation techniques. The team approach enables organizations to conduct an analysis of their supply chain, communicate with internal and external partners or stakeholders, and gain broad consensus regarding the appropriate resources for SCRM. The SCRM team consists of organizational personnel with diverse roles and responsibilities for leading and supporting SCRM activities, including risk executive, information technology, contracting, information security, privacy, mission or business, legal, supply chain and logistics, acquisition, business continuity, and other relevant functions. Members of the SCRM team are involved in various aspects of the SDLC and, collectively, have an awareness of and provide expertise in acquisition processes, legal practices, vulnerabilities, threats, and attack vectors, as well as an understanding of the technical aspects and dependencies of systems. The SCRM team can be an extension of the security and privacy risk management processes or be included as part of an organizational risk management team.

Related Controls: None.

References: [FASC18], [41 CFR 201], [EO 13873], [CNSSD 505], [SP 800-30], [SP 800-39], [SP-800-160-1], [SP 800-161], [SP 800-181], [IR 7622], [IR 8272].

SR-3 SUPPLY CHAIN CONTROLS AND PROCESSES

Control:

a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [*Assignment: organization-defined system or system component]* in coordination with [*Assignment: organization-defined supply chain personnel*];

b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: [*Assignment: organization-defined supply chain controls*]; and

c. Document the selected and implemented supply chain processes and controls in [*Selection: security and privacy plans; supply chain risk management plan;* [*Assignment: organization-defined document*]].

Discussion: Supply chain elements include organizations, entities, or tools employed for the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of systems and system components. Supply chain processes include hardware, software, and firmware development processes; shipping and handling procedures; personnel security and physical security programs; configuration management tools, techniques, and measures to maintain provenance; or other programs, processes, or procedures associated with the development, acquisition, maintenance and disposal of systems and system components. Supply chain elements and processes may be provided by organizations, system integrators, or external providers. Weaknesses or deficiencies in supply chain elements or processes represent potential vulnerabilities that can be exploited by adversaries to cause harm to the organization and affect its ability to carry out its core missions or business functions. Supply chain personnel are individuals with roles and responsibilities in the supply chain.

Related Controls: CA-2, MA-2, MA-6, PE-3, PE-16, PL-8, PM-30, SA-2, SA-3, SA-4, SA-5, SA-8, SA-9, SA-10, SA-15, SC-7, SC-29, SC-30, SC-38, SI-7, SR-6, SR-9, SR-11.

Control Enhancements:

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

(1) SUPPLY CHAIN CONTROLS AND PROCESSES | DIVERSE SUPPLY BASE

Employ a diverse set of sources for the following system components and services: [*Assignment: organization-defined system components and services*].

Discussion: Diversifying the supply of systems, system components, and services can reduce the probability that adversaries will successfully identify and target the supply chain and can reduce the impact of a supply chain event or compromise. Identifying multiple suppliers for replacement components can reduce the probability that the replacement component will become unavailable. Employing a diverse set of developers or logistics service providers can reduce the impact of a natural disaster or other supply chain event. Organizations consider designing the system to include diverse materials and components.

Related Controls: None.

(2) SUPPLY CHAIN PROTECTION CONTROLS AND PROCESSES | LIMITATION OF HARM

Employ the following controls to limit harm from potential adversaries identifying and targeting the organizational supply chain: [*Assignment: organization-defined controls*].

Discussion: Controls that can be implemented to reduce the probability of adversaries successfully identifying and targeting the supply chain include avoiding the purchase of custom or non-standardized configurations, employing approved vendor lists with standing reputations in industry, following pre-agreed maintenance schedules and update and patch delivery mechanisms, maintaining a contingency plan in case of a supply chain event, using procurement carve-outs that provide exclusions to commitments or obligations, using diverse delivery routes, and minimizing the time between purchase decisions and delivery.

Related Controls: None.

(3) SUPPLY CHAIN PROTECTION CONTROLS AND PROCESSES | SUB-TIER FLOW DOWN

Ensure that the controls included in the contracts of prime contractors are also included in the contracts of subcontractors.

Discussion: To manage supply chain risk effectively and holistically, it is important that organizations ensure that supply chain risk management controls are included at all tiers in the supply chain. This includes ensuring that Tier 1 (prime) contractors have implemented processes to facilitate the "flow down" of supply chain risk management controls to sub-tier contractors. The controls subject to flow down are identified in SR-3b.

Related Controls: SR-5, SR-8.

References: [FASC18], [41 CFR 201], [EO 13873], [ISO 20243], [SP 800-30], [SP 800-161], [IR 7622].

SR-4 PROVENANCE

Control: Document, monitor, and maintain valid provenance of the following systems, system components, and associated data: [*Assignment: organization-defined systems, system components, and associated data*].

Discussion: Every system and system component has a point of origin and may be changed throughout its existence. Provenance is the chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data. Organizations consider developing procedures (see SR-1) for allocating responsibilities for the creation, maintenance, and monitoring of provenance for systems and system components; transferring provenance documentation and responsibility between organizations; and preventing and monitoring for unauthorized changes to the provenance records. Organizations have methods to document, monitor, and maintain valid provenance baselines for systems, system components, and related data. These actions help track, assess,

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

and document any changes to the provenance, including changes in supply chain elements or configuration, and help ensure non-repudiation of provenance information and the provenance change records. Provenance considerations are addressed throughout the system development life cycle and incorporated into contracts and other arrangements, as appropriate.

Related Controls: CM-8, MA-2, MA-6, RA-9, SA-3, SA-8, SI-4.

Control Enhancements:

(1) PROVENANCE | IDENTITY

Establish and maintain unique identification of the following supply chain elements, processes, and personnel associated with the identified system and critical system components: [*Assignment: organization-defined supply chain elements, processes, and personnel associated with organization-defined systems and critical system components*].

Discussion: Knowing who and what is in the supply chains of organizations is critical to gaining visibility into supply chain activities. Visibility into supply chain activities is also important for monitoring and identifying high-risk events and activities. Without reasonable visibility into supply chains elements, processes, and personnel, it is very difficult for organizations to understand and manage risk and reduce their susceptibility to adverse events. Supply chain elements include organizations, entities, or tools used for the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of systems and system components. Supply chain processes include development processes for hardware, software, and firmware; shipping and handling procedures; configuration management tools, techniques, and measures to maintain provenance; personnel and physical security programs; or other programs, processes, or procedures associated with the production and distribution of supply chain elements. Supply chain personnel are individuals with specific roles and responsibilities related to the secure the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of a system or system component. Identification methods are sufficient to support an investigation in case of a supply chain change (e.g. if a supply company is purchased), compromise, or event.

Related Controls: IA-2, IA-8, PE-16.

(2) PROVENANCE | TRACK AND TRACE

Establish and maintain unique identification of the following systems and critical system components for tracking through the supply chain: [*Assignment: organization-defined systems and critical system components*].

Discussion: Tracking the unique identification of systems and system components during development and transport activities provides a foundational identity structure for the establishment and maintenance of provenance. For example, system components may be labeled using serial numbers or tagged using radio-frequency identification tags. Labels and tags can help provide better visibility into the provenance of a system or system component. A system or system component may have more than one unique identifier. Identification methods are sufficient to support a forensic investigation after a supply chain compromise or event.

Related Controls: IA-2, IA-8, PE-16, PL-2.

(3) PROVENANCE | VALIDATE AS GENUINE AND NOT ALTERED

Employ the following controls to validate that the system or system component received is genuine and has not been altered: [*Assignment: organization-defined controls*].

Discussion: For many systems and system components, especially hardware, there are technical means to determine if the items are genuine or have been altered, including optical and nanotechnology tagging, physically unclonable functions, side-channel analysis,

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

cryptographic hash verifications or digital signatures, and visible anti-tamper labels or stickers. Controls can also include monitoring for out of specification performance, which can be an indicator of tampering or counterfeits. Organizations may leverage supplier and contractor processes for validating that a system or component is genuine and has not been altered and for replacing a suspect system or component. Some indications of tampering may be visible and addressable before accepting delivery, such as inconsistent packaging, broken seals, and incorrect labels. When a system or system component is suspected of being altered or counterfeit, the supplier, contractor, or original equipment manufacturer may be able to replace the item or provide a forensic capability to determine the origin of the counterfeit or altered item. Organizations can provide training to personnel on how to identify suspicious system or component deliveries.

Related Controls: AT-3, SR-9, SR-10, SR-11.

(4) PROVENANCE | SUPPLY CHAIN INTEGRITY — PEDIGREE

Employ [*Assignment: organization-defined controls*] and conduct [*Assignment: organization-defined analysis*] to ensure the integrity of the system and system components by validating the internal composition and provenance of critical or mission-essential technologies, products, and services.

Discussion: Authoritative information regarding the internal composition of system components and the provenance of technology, products, and services provides a strong basis for trust. The validation of the internal composition and provenance of technologies, products, and services is referred to as the pedigree. For microelectronics, this includes material composition of components. For software this includes the composition of open-source and proprietary code, including the version of the component at a given point in time. Pedigrees increase the assurance that the claims suppliers assert about the internal composition and provenance of the products, services, and technologies they provide are valid. The validation of the internal composition and provenance can be achieved by various evidentiary artifacts or records that manufacturers and suppliers produce during the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of technology, products, and services. Evidentiary artifacts include, but are not limited to, software identification (SWID) tags, software component inventory, the manufacturers' declarations of platform attributes (e.g., serial numbers, hardware component inventory), and measurements (e.g., firmware hashes) that are tightly bound to the hardware itself.

Related Controls: RA-3.

References: [FASC18], [41 CFR 201], [EO 13873], [ISO 27036], [ISO 20243], [SP 800-160-1], [SP 800-161], [IR 7622], [IR 8112], [IR 8272].

SR-5 ACQUISITION STRATEGIES, TOOLS, AND METHODS

Control: Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [*Assignment: organization-defined acquisition strategies, contract tools, and procurement methods*].

Discussion: The use of the acquisition process provides an important vehicle to protect the supply chain. There are many useful tools and techniques available, including obscuring the end use of a system or system component, using blind or filtered buys, requiring tamper-evident packaging, or using trusted or controlled distribution. The results from a supply chain risk assessment can guide and inform the strategies, tools, and methods that are most applicable to the situation. Tools and techniques may provide protections against unauthorized production, theft, tampering, insertion of counterfeits, insertion of malicious software or backdoors, and poor development practices throughout the system development life cycle. Organizations also

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

consider providing incentives for suppliers who implement controls, promote transparency into their processes and security and privacy practices, provide contract language that addresses the prohibition of tainted or counterfeit components, and restrict purchases from untrustworthy suppliers. Organizations consider providing training, education, and awareness programs for personnel regarding supply chain risk, available mitigation strategies, and when the programs should be employed. Methods for reviewing and protecting development plans, documentation, and evidence are commensurate with the security and privacy requirements of the organization. Contracts may specify documentation protection requirements.

Related Controls: AT-3, SA-2, SA-3, SA-4, SA-5, SA-8, SA-9, SA-10, SA-15, SR-6, SR-9, SR-10, SR-11.

Control Enhancements:

(1) ACQUISITION STRATEGIES, TOOLS, AND METHODS | ADEQUATE SUPPLY

Employ the following controls to ensure an adequate supply of [*Assignment: organization-defined critical system components*]: [*Assignment: organization-defined controls*].

Discussion: Adversaries can attempt to impede organizational operations by disrupting the supply of critical system components or corrupting supplier operations. Organizations may track systems and component mean time to failure to mitigate the loss of temporary or permanent system function. Controls to ensure that adequate supplies of critical system components include the use of multiple suppliers throughout the supply chain for the identified critical components, stockpiling spare components to ensure operation during mission-critical times, and the identification of functionally identical or similar components that may be used, if necessary.

Related Controls: RA-9.

(2) ACQUISITION STRATEGIES, TOOLS, AND METHODS | ASSESSMENTS PRIOR TO SELECTION, ACCEPTANCE, MODIFICATION, OR UPDATE

Assess the system, system component, or system service prior to selection, acceptance, modification, or update.

Discussion: Organizational personnel or independent, external entities conduct assessments of systems, components, products, tools, and services to uncover evidence of tampering, unintentional and intentional vulnerabilities, or evidence of non-compliance with supply chain controls. These include malicious code, malicious processes, defective software, backdoors, and counterfeits. Assessments can include evaluations; design proposal reviews; visual or physical inspection; static and dynamic analyses; visual, x-ray, or magnetic particle inspections; simulations; white, gray, or black box testing; fuzz testing; stress testing; and penetration testing (see SR-6(1)). Evidence generated during assessments is documented for follow-on actions by organizations. The evidence generated during the organizational or independent assessments of supply chain elements may be used to improve supply chain processes and inform the supply chain risk management process. The evidence can be leveraged in follow-on assessments. Evidence and other documentation may be shared in accordance with organizational agreements.

Related Controls: CA-8, RA-5, SA-11, SI-7.

References: [FASC18], [41 CFR 201], [EO 13873], [ISO 27036], [ISO 20243], [SP 800-30], [SP 800-161], [IR 7622], [IR 8272].

SR-6 SUPPLIER ASSESSMENTS AND REVIEWS

Control: Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [*Assignment: organization-defined frequency*].

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

Discussion: An assessment and review of supplier risk includes security and supply chain risk management processes, foreign ownership, control or influence (FOCI), and the ability of the supplier to effectively assess subordinate second-tier and third-tier suppliers and contractors. The reviews may be conducted by the organization or by an independent third party. The reviews consider documented processes, documented controls, all-source intelligence, and publicly available information related to the supplier or contractor. Organizations can use open-source information to monitor for indications of stolen information, poor development and quality control practices, information spillage, or counterfeits. In some cases, it may be appropriate or required to share assessment and review results with other organizations in accordance with any applicable rules, policies, or inter-organizational agreements or contracts.

Related Controls: SR-3, SR-5.

Control Enhancements:

(1) SUPPLIER ASSESSMENTS AND REVIEWS | TESTING AND ANALYSIS

Employ [*Selection (one or more): organizational analysis; independent third-party analysis; organizational testing; independent third-party testing*] of the following supply chain elements, processes, and actors associated with the system, system component, or system service: [*Assignment: organization-defined supply chain elements, processes, and actors*].

Discussion: Relationships between entities and procedures within the supply chain, including development and delivery, are considered. Supply chain elements include organizations, entities, or tools that are used for the research and development, design, manufacturing, acquisition, delivery, integration, operations, maintenance, and disposal of systems, system components, or system services. Supply chain processes include supply chain risk management programs; SCRM strategies and implementation plans; personnel and physical security programs; hardware, software, and firmware development processes; configuration management tools, techniques, and measures to maintain provenance; shipping and handling procedures; and programs, processes, or procedures associated with the production and distribution of supply chain elements. Supply chain actors are individuals with specific roles and responsibilities in the supply chain. The evidence generated and collected during analyses and testing of supply chain elements, processes, and actors is documented and used to inform organizational risk management activities and decisions.

Related Controls: CA-8, SI-4.

References: [FASC18], [41 CFR 201], [EO 13873], [ISO 27036], [ISO 20243], [FIPS 140-3], [FIPS 180-4], [FIPS 186-4], [FIPS 202], [SP 800-30], [SP 800-161], [IR 7622], [IR 8272].

SR-7 SUPPLY CHAIN OPERATIONS SECURITY

Control: Employ the following Operations Security (OPSEC) controls to protect supply chain-related information for the system, system component, or system service: [*Assignment: organization-defined Operations Security (OPSEC) controls*].

Discussion: Supply chain OPSEC expands the scope of OPSEC to include suppliers and potential suppliers. OPSEC is a process that includes identifying critical information, analyzing friendly actions related to operations and other activities to identify actions that can be observed by potential adversaries, determining indicators that potential adversaries might obtain that could be interpreted or pieced together to derive information in sufficient time to cause harm to organizations, implementing safeguards or countermeasures to eliminate or reduce exploitable vulnerabilities and risk to an acceptable level, and considering how aggregated information may expose users or specific uses of the supply chain. Supply chain information includes user identities; uses for systems, system components, and system services; supplier identities; security and privacy requirements; system and component configurations; supplier processes; design specifications; and testing and evaluation results. Supply chain OPSEC may require

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

organizations to withhold mission or business information from suppliers and may include the use of intermediaries to hide the end use or users of systems, system components, or system services.

Related Controls: SC-38.

Control Enhancements: None.

References: [EO 13873], [SP 800-30], [ISO 27036], [SP 800-161], [IR 7622].

SR-8 NOTIFICATION AGREEMENTS

Control: Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [*Selection (one or more): notification of supply chain compromises; results of assessments or audits;* [*Assignment: organization-defined information*]].

Discussion: The establishment of agreements and procedures facilitates communications among supply chain entities. Early notification of compromises and potential compromises in the supply chain that can potentially adversely affect or have adversely affected organizational systems or system components is essential for organizations to effectively respond to such incidents. The results of assessments or audits may include open-source information that contributed to a decision or result and could be used to help the supply chain entity resolve a concern or improve its processes.

Related Controls: IR-4, IR-6, IR-8.

Control Enhancements: None.

References: [FASC18], [41 CFR 201], [EO 13873], [ISO 27036], [SP 800-30], [SP 800-161], [IR 7622].

SR-9 TAMPER RESISTANCE AND DETECTION

Control: Implement a tamper protection program for the system, system component, or system service.

Discussion: Anti-tamper technologies, tools, and techniques provide a level of protection for systems, system components, and services against many threats, including reverse engineering, modification, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting systems and components during distribution and when in use.

Related Controls: PE-3, PM-30, SA-15, SI-4, SI-7, SR-3, SR-4, SR-5, SR-10, SR-11.

Control Enhancements:

(1) TAMPER RESISTANCE AND DETECTION | MULTIPLE STAGES OF SYSTEM DEVELOPMENT LIFE CYCLE

Employ anti-tamper technologies, tools, and techniques throughout the system development life cycle.

Discussion: The system development life cycle includes research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal. Organizations use a combination of hardware and software techniques for tamper resistance and detection. Organizations use obfuscation and self-checking to make reverse engineering and modifications more difficult, time-consuming, and expensive for adversaries. The customization of systems and system components can make substitutions easier to detect and therefore limit damage.

Related Controls: SA-3.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

References: [ISO 20243].

SR-10 INSPECTION OF SYSTEMS OR COMPONENTS

Control: Inspect the following systems or system components [*Selection (one or more): at random;* at [*Assignment: organization-defined frequency*], *upon* [*Assignment: organization-defined indications of need for inspection*]] to detect tampering: [*Assignment: organization-defined systems or system components*].

Discussion: The inspection of systems or systems components for tamper resistance and detection addresses physical and logical tampering and is applied to systems and system components removed from organization-controlled areas. Indications of a need for inspection include changes in packaging, specifications, factory location, or entity in which the part is purchased, and when individuals return from travel to high-risk locations.

Related Controls: AT-3, PM-30, SI-4, SI-7, SR-3, SR-4, SR-5, SR-9, SR-11.

References: [ISO 20243].

SR-11 COMPONENT AUTHENTICITY

Control:

a. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and

b. Report counterfeit system components to [*Selection (one or more): source of counterfeit component;* [*Assignment: organization-defined external reporting organizations*]*;* [*Assignment: organization-defined personnel or roles*]].

Discussion: Sources of counterfeit components include manufacturers, developers, vendors, and contractors. Anti-counterfeiting policies and procedures support tamper resistance and provide a level of protection against the introduction of malicious code. External reporting organizations include CISA.

Related Controls: PE-3, SA-4, SI-7, SR-9, SR-10.

Control Enhancements:

(1) COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT TRAINING

Train [*Assignment: organization-defined personnel or roles*] to detect counterfeit system components (including hardware, software, and firmware).

Discussion: None.

Related Controls: AT-3.

(2) COMPONENT AUTHENTICITY | CONFIGURATION CONTROL FOR COMPONENT SERVICE AND REPAIR

Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: [*Assignment: organization-defined system components*].

Discussion: None.

Related Controls: CM-3, MA-2, MA-4, SA-10.

(3) COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT SCANNING

Scan for counterfeit system components [*Assignment: organization-defined frequency*].

Discussion: The type of component determines the type of scanning to be conducted (e.g., web application scanning if the component is a web application).

Related Controls: RA-5.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5

References: [ISO 20243].

SR-12 COMPONENT DISPOSAL

Control: Dispose of [*Assignment: organization-defined data, documentation, tools, or system components*] using the following techniques and methods: [*Assignment: organization-defined techniques and methods*].

Discussion: Data, documentation, tools, or system components can be disposed of at any time during the system development life cycle (not only in the disposal or retirement phase of the life cycle). For example, disposal can occur during research and development, design, prototyping, or operations/maintenance and include methods such as disk cleaning, removal of cryptographic keys, partial reuse of components. Opportunities for compromise during disposal affect physical and logical data, including system documentation in paper-based or digital files; shipping and delivery documentation; memory sticks with software code; or complete routers or servers that include permanent media, which contain sensitive or proprietary information. Additionally, proper disposal of system components helps to prevent such components from entering the gray market.

Related Controls: MP-6.

References: None.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53r5