From: 800-171comments@list.nist.gov on behalf of [redacted]
To: 800-171comments@list.nist.gov
Cc: [redacted]
Subject: [800-171 Comments] Comments on Updates to NIST 800-172 From the SEI and JHUAPL
Date: Thursday, October 17, 2024 7:19:00 PM
Attachments: Proposed 800-172 update-Comment w Rationale & Purpose v3 F.pdf
Proposed 800-172 update-Requirements by Family v4 F.pdf
NIST.SP.800-172 Proposed Descriptions Updates SEI JHUAPL.pdf

Attached are combined comments from the SEI and JHUAPL on proposed updates to NIST SP 800-172 based on NIST 800-53 R5 in support of NIST 800-171 R3. We have used the NIST Comment format in the attached PDF file "Proposed 800-172 update-Comment w Rationale..." to summarize our proposed updates. Detailed proposed Requirement updates are in the attached PDF "...update-Requirements by Family"

800-172 is currently based on revision 4 of 800-53. The release of the updated 800-171 r3 which is based on 800-53 r5 has several enhancements that suggest an update to 800-172 is merited. We are proposing additional Requirements be included in an update to 800-172. These refinements would be valuable to support the management of security and privacy in situations where advanced persistent threats (APT) may be a material risk to availability, integrity, and confidentiality. Each recommendation is labeled (column A) in the "Proposed 800-172 updates..." PDF with a Purpose, e.g., Gap, Incremental enhancement, or an Enhancement.

For areas identified as Gaps (e.g., PL, MP, SA, SR, CP) under "Purpose" in the attached proposed update table C-2 we have developed drafts of the Descriptions for those Requirements/controls. Those Description suggestions are included in the attached PDF "... Proposed Descriptions..." file.

Regards,

Charles M. Wallen
CERT | Software Engineering Institute |Carnegie Mellon University
[redacted]

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
1	CMU - SEI & JHUAPL		NIST 800 - 171 R3, 800-53 R5, and 800-172	800-172 Chapter 3 The Requirements on pg 11 and Appendix C Mapping Tables on pg 50	NA	800-172 is currently based on revision 4 of 800-53. The release of the updated 800-171 r3 which is based on 800-53 r5 has several enhancements that suggest an update to 800-172 is merited. We are proposing additional Requirements be included in an update to 800-172. These refinements would be valuable to support the management of security and privacy in situations where advanced persistent threats (APT) may be a material risk to availability, integrity, and confidentiality. Each recommendation is labeled (column A) in the 800-172 "Proposed updates w Purp" spreadsheet in this Excel Workbook with a Purpose, e.g., address a Gap, Incremental enhancement, or an Enhancement to the existing 800-172 Requirements.	***Update 800-172 with additional Requirements to more effectively address NIST 800-53 R5 revisions and support NIST 800-171 R3:*** Add four 800-53 controls to Access, AC-2 (12) Account Monitoring for Atypical Usage, AC-3 (13) Attribute-Based Access Control, AC-18 (3) Disable Wireless Access When Not Intended for Use, AC-17 (01) Remote Access Monitoring and Control.
2	CMU - SEI & JHUAPL		See Comment 1	See Comment 1	NA	see Comment 1	Add two 800-53 controls to Audit and Accountability, AU- (05) Integrated Analysis of Audit Records, A9-3 (02) Protect and Store Audit Information in a Repository on a Separate System.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
3	CMU - SEI & JHUAPL		See Comment 1	See Comment 1	NA	see Comment 1	Add two 800-53 controls to Incident Response, IR-4 (11) Integrated Incidence Response Team, IR-4 (13) Behavioral Analysis.
4	CMU - SEI & JHUAPL		See Comment 1	See Comment 1	NA	see Comment 1	Add four 800-53 controls to System and Communication Protection, SC-41 Port and I/O Device Access, SC-07 (04) Boundary Protection - External Telecommunications Services, SC-44 Detonation Chamber/Sandboxing, SC-28 (01) Protection of Information at Rest - Cryptographic Protection.
5	CMU - SEI & JHUAPL		See Comment 1	See Comment 1	NA	see Comment 1	Add one 800-53 control to Program Management, PM-16 Threat Intelligence Program.
6	CMU - SEI & JHUAPL		See Comment 1	800-171 R3 Table 1 on page 4	NA	see Comment 1	Add Program Management as Family #19.
7	CMU - SEI & JHUAPL		See Comment 1	See Comment 1	NA	see Comment 1	Add one 800-53 control to System and Information Integrity, SI-4 (24) System Monitoring - Indicators of Compromise .
8	CMU - SEI & JHUAPL		See Comment 1	See Comment 1	NA	see Comment 1	Add one 800-53 control to Risk Assessment, RA-02 Security Categorization .
9	CMU - SEI & JHUAPL		See Comment 1	See Comment 1	NA	see Comment 1	Add two 800-53 controls to the Planning, PL 08 security and privacy architecturee and PL 08(01) defense in depth.

Comment #	Submitted By (Name/Org):*	Type (General / Editorial / Technical)	Source (publication, analysis, overlay)	Starting Page # *	Starting Line #*	Comment (include rationale)*	Suggested Change*
10	CMU - SEI & JHUAPL		See Comment 1	See Comment 1	NA	see Comment 1	Add one 800-53 control to Media Protection, Cryptographic Protection CP-09 (08). Currently this control is proposed as a requirement for 800-173 r3. We believe this control may be better aligned as an Enhanced Control in 800-172.
11	CMU - SEI & JHUAPL		See Comment 1	See Comment 1	NA	see Comment 1	Add four 800-53 controls to the System and Services Acquisition, SA-03 System Development Lifecycle, SA-04 Acquisition Process, SA-04(05) System Component and Service Configuration, and SA 05 System Documentation
12	CMU - SEI & JHUAPL		See Comment 1	See Comment 1	NA	see Comment 1	Add one 800-53 control to Supply Chain Risk Management, SR-08 Notification Agreements
13	CMU - SEI & JHUAPL		See Comment 1	See Comment 1	NA	see Comment 1	Add eleven 800-53 controls to Contingency Planning , including: Policy and Procedures CP-01, Plan CP-02, Coordinate w Ext Provider CP-02 (07), ID Assets CP-02 (08), Testing CP-04, Alt Storage CP-06, RTO-RPO CP-06 (02), Alt Processing CP-07, Telcom CP-08, CP-09 (01) Testing for Reliability, System Recovery CP-10
14	CMU - SEI & JHUAPL		See Comment 1	800-171 R3 Table 1 on page 4	NA	see Comment 1	Add Contingency Planning as Family # 18

SP 800 - 172 w Proposed Updates to Support 800 - 173 R3, and 800-53 R5

Enhanced Security Requirements fo Protecting CUI - Table C-2

Purpose

Purpose	SECURITY REQUIREMENTS	Defense-in-Depth Protection Strategy			NIST SP 800-53 *Relevant Security Controls*	
		PRA	DLO	CRS		
	Access (AC) - Proposed					
Incremental Enhancement	3.01.04e Monitor and report organization defined atypcal usage of system accounts				AC-2 (12)	Account Monitoring for Atypical Usage
Incremental Enhancement	3.01.05e Enforce organization defined subject/object attribute-based access control policy				AC-3 (13)	Attribute-Based Access Control
Enhancement	3.01.06e Disable wireless capabilities when not needed for essential organizational missions to reduce susceptibility to threats				AC-18 (3)	Disable Wireless Access When Not Intended for Use
Enhancement	3.01.07e Employ automated mechanisms to monitor and control remote access methods.				AC-17 (01)	Remote Access Monitoring and Control

Purpose	SECURITY REQUIREMENTS	Defense-in-Depth Protection Strategy	NIST SP 800-53 *Relevant Security Controls*

		PRA	DLO	CRS		
	Audit and Accountabiliy (AU) - Proposed					
Incremental Enhancement	3.03.09e Integrate analysis of audit records with multiple organization-defined data/information/systems to further enhance the ability to identify inappropriate or unusual activity.				AU-6 (05)	Integrated Analysis of Audit Records
Incremental Enhancement	3.03.10e Store audit records in a repository that is part of a physically different system or system component than the system or component being audited.				AU-9 (02)	Protect and Store Audit Information in a Repository on a Separate System

Purpose	SECURITY REQUIREMENTS	Defense-in-Depth Protection Strategy			NIST SP 800-53 *Relevant Security Controls*
		PRA	DLO	CRS	
	Incident Response (IR) - Proposed				

Enhancement	3.06.06e Integrated incident response team leverage team knowledge of the threat and implement measures that promote the rapid detection of intrusions, the development of appropriate mitigations, and the deployment of effective defensive measures. These teams can identify adversary tactics, techniques, and procedures that to define a more effective response.				IR-4 (11)	Integrated Incident Response Team
Incremental Enhancement	3.06.07e Analyze anomalous or suspected adversarial behavior in or related to organization-defined environments.				IR-4 (13)	Behavioral Analysis

SECURITY REQUIREMENTS	Defense-in-Depth Protection Strategy			NIST SP 800-53 *Relevant Security Controls*	
	PRA	DLO	CRS		
Purpose	**System and Communication Protection (SC) - Proposed**				
Enhancement	3.13.06e Physically/ logically identify and disable or remove organization-defined connection ports or input/output devices on systems or system components.			SC-41	Port and I/O Device Access

Incremental Enhancement	3.13.07e Implement a managed interface for each external telecommunication service and prevent unauthorized exchange of control plane traffic with external networks.				SC-07 ((04)	Boundary Protection - External Telecommunications Services
Enhancement	3.13.08 Allow organizations to open email attachments, execute untrusted or suspicious applications in the safety of an isolated environment or sandbox.				SC-44	Detonation Chamber/Sandboxing
Enhancement	3.13.09 Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of organization-defined information.				SC-28 (01)	Protection of Information at Rest - Cryptographic Protection

SECURITY REQUIREMENTS		Defense-in-Depth Protection Strategy			NIST SP 800-53 *Relevant Security Controls*
		PRA	DLO	CRS	
Purpose	**Program Management (PM) - Proposed; would also add Family (#19) to 172 list**				
Incremental Enhancement	3.19.03e Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.				PM-16	Threat Intelligence Program

SECURITY REQUIREMENTS	Defense-in-Depth Protection Strategy			NIST SP 800-53 *Relevant Security Controls*	
	PRA	DLO	CRS		
Purpose	**System and Information Integrity (SI) - Proposed**				
Incremental Enhancement	3.14.08e Discover, collect, and distribute indicators of compromise.			SI-4(24)	System Monitoring - Indicators of Compromise

Purpose	SECURITY REQUIREMENTS	Defense-in-Depth Protection Strategy			NIST SP 800-53 *Relevant Security Controls*
		PRA	DLO	CRS	
	Risk Assessment (RA) - Proposed				

Incremental Enancement	3.11.08e Categorize the system and information it processes, stores, and transmits. Security categories describe the potential adverse impacts or negative consequences if organizational information and systems are compromised through a loss of confidentiality, integrity, or availability.				RA-02	Security Categorization

Purpose	SECURITY REQUIREMENTS	Defense-in-Depth Protection Strategy			NIST SP 800-53 *Relevant Security Controls*	
		PRA	DLO	CRS		
	Planning (PL) - Proposed					
Gap	3.15.04e Develop and manage security/privacy architectures for the system that describe the requirements for CIA and PII that integrate with the				PL-08	Security and Privacy Architectures
Gap	3.15.05e Design security/privacy system architectures using defense in depth methods that ensure controls operate in a coordinated and mutually reinforcing manner.				PL -08 (1)	Defense in Depth Architectures

Media Protection (MP) - Proposed

Purpose	SECURITY REQUIREMENTS	Defense-in-Depth Protection Strategy			NIST SP 800-53 Relevant Security Controls
		PRA	DLO	CRS	
Gap	3.08.09e Conduct backups of user, system, key security/system/procedural documentation, and protect the confidentiality, integrity and availability of system information				CP-09 (08) System Backup - Cryptographic Protection
	~~There are no enhanced security requirements for media protection.~~				

System and Services Acquisition (SA) - Proposed

Purpose	SECURITY REQUIREMENTS	Defense-in-Depth Protection Strategy			NIST SP 800-53 Relevant Security Controls
		PRA	DLO	CRS	

Gap	3.16.04e Acquire, develop, and manage systems using methods that fully addresses security/privacy requirements beginning in the earliest stages of planning through operations and disposal.				SA 03	System development lifecycle
Gap	3.16.05e Include requirements, descriptions, criteria, and roles-accountabilities for systems across their lifecycle in contracts for HW, SW, and services.				SA 04	Acquisition Process
Gap	3.16.06e Require system developers and suppliers to implement managed configurations that leverage secure baselines for functions, ports, protocols, and services.				SA 04 (05)	System, component, and service configurations
Gap	3.16.07e Obtain, develop, distribute, and administer security/privacy oriented system documentation for all components, services, and individuals.				SA 05	System documentation

Purpose

Supply Chain Risk Management (SR) - Proposed

SECURITY REQUIREMENTS	Defense-in-Depth Protection Strategy			NIST SP 800-53 Relevant Security Controls
	PRA	DLO	CRS	

Gap	3.17.04e Establish agreements and procedures with suppliers of systems, components, and services that require notification of compromises or potential compromises - vulnerabilities, and facilitates communication.				SR-08	Notification Agreements

Contingency Planning (CP) - Proposed

Purpose	SECURITY REQUIREMENTS	Defense-in-Depth Protection Strategy			NIST SP 800-53 *Relevant Security Controls*	
		PRA	DLO	CRS		
Gap	3.15.01e Develop, document, and disseminate policy and procedures for Contingency Planning				CP-01	Policy and Procedures
Gap	3.15.02e Develop, document, and disseminate contingency plans and procedures				CP-02	Contingency Plan
Gap	3.18.03e Coordinate contingency plans with service providers to support contingency requirements				CP-02 (07)	Coordinate with Exernal Service Providers
Gap	3.18.04e Identify critical system assets that support essential functions				CP-02 (08)	Identify Critical Assets

Gap	3.18.05e Test system contingency plans, review results, and improve plans as needed				CP-04	Contingency Plan Testing
Gap	3.18.06eEstablish alternate storage site(s) to facilitate the retrieval/recovery of information and data				CP-06	Alternate Storage Site
Gap	3.18.07e Configure the alternate storage site to achieve system recovery (s) that meets the RTO and RPO				CP-06 (02)	Alternate Storage Site - Recovery Time (RTO) and Recovery Point (RPO) Objectives
Gap	3.18.08e Establish alternate processing site(s) to facilitate the processing of information and data in a manner that meets the RTO and RPO of the system(s)				CP-07	Alternate Processing Site
Gap	3.18.09e Establish alternate telecommunication service capabilities that meet the voice and data requirements of the organization and its systems				CP-08	Telecommunications Services
Gap	3.18.10e Test the capability and reliability of systems/components to retrieve information/media to meet RTO and RTO.				CP-09 (01)	. Testing for Reliability and Integrity
Gap	3.18.11e Provide for the recovery and reconstitution of the system(s) to a known state within the RTO and RPO objective timeframes.				CP-10	System Recovery and Reconstitution

NIST Special Publication 800-172

Proposed Additional Enhanced Security Requirements for Protecting Controlled Unclassified Information NIST 800-172

A Supplement to NIST Special Publication 800-171 R3 update based on 800-53 r5_

Carnegie Mellon SEI and JHUAPL Proposed Updates - October 2024

Proposed Families - Table 1. Security Requirement Families – 19

Contingency Planning – a proposed addition

Access Control	Maintenance	System and Communications Protection
Awareness and Training	Media Protection	System and Information Integrity
Audit and Accountability	Personnel Security	Planning
Configuration Management	Physical Protection	System and Services Acquisition
Identification and Authentication	Risk Assessment	Supply Chain Risk Management
Incident Response	Security Assessment and Monitoring	***Contingency Planning*** ***Program Management***

CHAPTER THREE additions to 800-172. No enhanced controls were removed from the previous version released in February 2021. One key group of additional 800-53 controls is a new series of practices addressing largely availability in a new proposed Continuity Planning family.

3.1 Media Protection - Proposed

Enhanced Security Requirements

3.08.09e **Conduct backups of user, system, key security/system/procedural documentation, and protect the system information with cryptographic mechanisms.**

DISCUSSION

Discussion: The selection of cryptographic mechanisms is based on the need to protect the confidentiality and integrity of backup information. The strength of mechanisms selected is commensurate with the security category or classification of the information. Cryptographic protection applies to system backup information in storage at both primary and alternate locations. Organizations that implement cryptographic mechanisms to protect information at rest also consider cryptographic key management solutions.

Related Controls: SC-12, SC-13, SC-28.

3.2 Planning - Proposed

Enhanced Security Requirements

3.15.04e **Develop and manage security/privacy architectures for the system that describe the requirements for CIA and PII that integrate with the enterprise architecture, including any external systems/services.**

DISCUSSION

Security and privacy architectures should be designed to ensure that the system integrates with or are tightly coupled to the enterprise architecture. The architectures include an architectural description, the allocation of security and privacy functionality (including controls), security- and privacy-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. The architectures can also

include other information, such as user roles and the access privileges assigned to each role; security and privacy requirements; types of information processed, stored, and transmitted by the system; supply chain risk management requirements; restoration priorities of information and system services; and other protection needs.

In today's modern computing architectures, it is becoming less common for organizations to control all information resources. There may be key dependencies on external information services and service providers. Describing such dependencies in the security and privacy architectures is necessary for developing a comprehensive mission and business protection strategy. Establishing, developing, documenting, and maintaining under configuration control a baseline configuration for organizational systems is critical to implementing and maintaining effective architectures. The development of the architectures is coordinated with the senior agency information security officer and the senior agency official for privacy to ensure that the controls needed to support security and privacy requirements are identified and effectively implemented. In many circumstances, there may be no distinction between the security and privacy architecture for a system. In other circumstances, security objectives may be adequately satisfied, but privacy objectives may only be partially satisfied by the security requirements. In these cases, consideration of the privacy requirements needed to achieve satisfaction will result in a distinct privacy architecture. The documentation, however, may simply reflect the combined architectures.

Related Controls: CM-2, CM-6, PL-2, PL-7, PL-9, PM-5, PM-7, RA-9, SA-3, SA-5, SA-8, SA-17, SC-7.

3.15.05e **Design security/privacy system architectures using defense in depth methods that ensure controls operate in a coordinated and mutually reinforcing manner.**

DISCUSSION

Security Organizations strategically allocate security and privacy controls in the security and privacy architectures so that adversaries must overcome multiple controls to achieve their objective. Requiring adversaries to defeat multiple controls makes it more difficult to attack information resources by increasing the work factor of the adversary; it also increases the likelihood of detection. The coordination of allocated controls is essential to ensure that an attack that involves one control does not create adverse, unintended consequences by interfering with other controls. Unintended consequences can include system lockout and cascading alarms. The placement of controls in systems and organizations is an important activity that requires thoughtful analysis. The value of organizational assets is an important consideration in providing additional layering. Defense-in-depth architectural approaches include modularity and layering, separation of system and user functionality, and security function isolation.

Related Controls: SC-2, SC-3, SC-29, SC-36.

3.3 System and Services Acquisition (SA) - Proposed

Enhanced Security Requirements

3.16.04e **Acquire, develop, and manage systems using methods that fully addresses security/privacy requirements beginning in the earq liest stages of planning through operations and disposal.**

DISCUSSION

The establishment A system development life cycle process provides the foundation for the successful development, implementation, and operation of organizational systems. The integration of security and privacy considerations early in the system development life cycle is a foundational principle of systems security engineering and privacy engineering. To apply the required controls within the system development life cycle requires a basic understanding of information security and privacy, threats, vulnerabilities, adverse impacts, and risk to critical mission and business functions. The security engineering principles help individuals properly design, code, and test systems and system components. Organizations include qualified personnel (e.g., senior agency information security officers, senior agency officials for privacy, security and privacy architects, and security and privacy engineers) in system development life cycle processes to ensure

that established security and privacy requirements are incorporated into organizational systems. Role-based security and privacy training programs can ensure that individuals with key security and privacy roles and responsibilities have the experience, skills, and expertise to conduct assigned system development life cycle activities.

The effective integration of security and privacy requirements into enterprise architecture also helps to ensure that important security and privacy considerations are addressed throughout the system life cycle and that those considerations are directly related to organizational mission and business processes. This process also facilitates the integration of the information security and privacy architectures into the enterprise architecture, consistent with the risk management strategy of the organization. Because the system development life cycle involves multiple organizations, (e.g., external suppliers, developers, integrators, service providers), acquisition and supply chain risk management functions and controls play significant roles in the effective management of the system during the life cycle.

Related Controls: AT-3, PL-8, PM-7, SA-4, SA-5, SA-8, SA-11, SA-15, SA-17, SA-22, SR-3, SR-4, SR-5, SR-9.

3.16.05e Include requirements, descriptions, criteria, and roles-accountabilities for systems across their lifecycle in contracts for HW, SW, and services.

DISCUSSION

The Security and privacy functional requirements are typically derived from the high-level security and privacy requirements. The derived requirements include security and privacy capabilities, functions, and mechanisms. Strength requirements associated with such capabilities, functions, and mechanisms include degree of correctness, completeness, resistance to tampering or bypass, and resistance to direct attack. Assurance requirements include development processes, procedures, and methodologies as well as the evidence from development and assessment activities that provide grounds for confidence that the required functionality is implemented and possesses the required strength of mechanism. [SP 800-160-1] describes the process of requirements engineering as part of the system development life cycle.

Controls can be viewed as descriptions of the safeguards and protection capabilities appropriate for achieving the particular security and privacy objectives of the organization and for reflecting the security and privacy requirements of stakeholders. Controls are selected and implemented in order to satisfy system requirements and include developer and organizational responsibilities. Controls can include technical, administrative, and physical aspects. In some cases, the selection and implementation of a control may necessitate additional specification by the organization in the form of derived requirements or instantiated control parameter values. The derived requirements and control parameter values may be necessary to provide the appropriate level of implementation detail for controls within the system development life cycle.

Security and privacy documentation requirements address all stages of the system development lifecycle. Documentation provides user and administrator guidance for the implementation and operation of controls. The level of detail required in such documentation is based on the security categorization or classification level of the system and the degree to which organizations depend on the capabilities, functions, or mechanisms to meet risk response expectations. Requirements can include mandated configuration settings that specify allowed functions, ports, protocols, and services. Acceptance criteria for systems, system components, and system services are defined in the same manner as the criteria for any organizational acquisition or procurement.

3.16.06e Require system developers and suppliers to implement managed configurations that leverage secure baselines for functions, ports, protocols, and services.

DISCUSSION

Management of configurations in a secure consistent manner is an essential practice to help ensure the security and privacy of systems and the information they store and process. Examples of security configurations include the U.S. Government Configuration Baseline (USGCB), Security Technical Implementation Guides (STIGs), and any limitations on functions, ports, protocols, and services. Security characteristics can include requiring that default passwords have been changed.

Related Controls: None.

3.16.07e Obtain, develop, distribute, and administer security/privacy oriented system documentation for all components, services, and individuals.

DISCUSSION
System documentation helps personnel understand the implementation and operation of controls. Organizations consider establishing specific measures to determine the quality and completeness of the content provided. System documentation may be used to support the management of supply chain risk, incident response, and other functions. Personnel or roles that require documentation include system owners, system security officers, and system administrators. Attempts to obtain documentation include contacting manufacturers or suppliers and conducting web-based searches. The inability to obtain documentation may occur due to the age of the system or component or the lack of support from developers and contractors. When documentation cannot be obtained, organizations may need to recreate the documentation if it is essential to the implementation or operation of the controls. The protection provided for the documentation is commensurate with the security category or classification of the system. Documentation that addresses system vulnerabilities may require an increased level of protection. Secure operation of the system includes initially starting the system and resuming secure system operation after a lapse in system operation.

Related Controls: CM-4, CM-6, CM-7, CM-8, PL-2, PL-4, PL-8, PS-2, SA-3, SA-4, SA-8, SA-9, SA-10, SA-11, SA-15, SA-16, SA-17, SI-12, SR-3.

3.4 Supply Chain Risk Management (SR) – Proposed

Enhanced Security Requirements

3.17.04e Establish agreements and procedures with suppliers of systems, components, and services that require notification of compromises or potential compromises - vulnerabilities, and facilitates communication

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.

3.5 Contingency Planning (CP) - Proposed

Enhanced Security Requirements

3.15.01e Develop, document, and disseminate policy and procedures for Contingency Planning

DISCUSSION
Contingency planning policy and procedures address the controls in the CP family 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 contingency planning 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 contingency planning policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

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

3.15.02e Develop, document, and disseminate contingency plans and procedures

DISCUSSION

Contingency planning for systems is part of an overall program for achieving continuity of operations for organizational mission and business functions. Contingency planning addresses system restoration and implementation of alternative mission or business processes when systems are compromised or breached. Contingency planning is considered throughout the system development life cycle and is a fundamental part of the system design. Systems can be designed for redundancy, to provide backup capabilities, and for resilience. Contingency plans reflect the degree of restoration required for organizational systems since not all systems need to fully recover to achieve the level of continuity of operations desired. System recovery objectives reflect applicable laws, executive orders, directives, regulations, policies, standards, guidelines, organizational risk tolerance, and system impact level.

Actions addressed in contingency plans include orderly system degradation, system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By coordinating contingency planning with incident handling activities, organizations ensure that the necessary planning activities are in place and activated in the event of an incident. Organizations consider whether continuity of operations during an incident conflicts with the capability to automatically disable the system. Incident response planning is part of contingency planning for organizations and is addressed in the NIST 800-53 Incident Response family.

Related Controls: CP-3, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11, CP-13, IR-4, IR-6, IR-8, IR-9, MA-6, MP-2, MP-4, MP-5, PL-2, PM-8, PM-11, SA-15, SA-20, SC-7, SC-23, SI-12.

3.18.03e Coordinate the contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.

DISCUSSION

When the capability of an organization to carry out its mission and business functions is dependent on external service providers, developing a comprehensive and timely contingency plan may become more challenging. When mission and business functions are dependent on external service providers, organizations coordinate contingency planning activities with the external entities to ensure that the individual plans reflect the overall contingency needs of the organization.

Related Controls: SA-9.

3.18.04e Identify critical system assets that support essential functions

DISCUSSION

Organizations may choose to identify critical assets as part of criticality analysis, business continuity planning, or business impact analyses. Organizations identify critical system assets so that additional controls can be employed (beyond the controls routinely implemented) to help ensure that organizational mission and business functions can continue to be conducted during contingency operations. The identification of critical information assets also facilitates the prioritization of organizational resources. Critical system assets include

technical and operational aspects. Technical aspects include system components, information technology services, information technology products, and mechanisms. Operational aspects include procedures (i.e., manually executed operations) and personnel (i.e., individuals operating technical controls and/or executing manual procedures). Organizational program protection plans can assist in identifying critical assets. If critical assets are resident within or supported by external service providers, organizations consider coordination of contingency plans with the service provider(s) as a control enhancement.

Related Controls: CM-8, RA-9.

3.18.05e Test system contingency plans, review results, and improve plans as needed

DISCUSSION
Methods for testing contingency plans to determine the effectiveness of the plans and identify potential weaknesses include checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), and comprehensive exercises. Organizations conduct testing based on the requirements in contingency plans and include a determination of the effects on organizational operations, assets, and individuals due to contingency operations. Organizations have flexibility and discretion in the breadth, depth, and timelines of corrective actions.

Related Controls: AT-3, CP-2, CP-3, CP-8, CP-9, IR-3, IR-4, PL-2, PM-14, SR-2.

3.18.06e Establish alternate storage site(s) to facilitate the retrieval/recovery of information and data

DISCUSSION
Alternate storage sites are geographically distinct from primary storage sites and maintain duplicate copies of information and data if the primary storage site is not available. Similarly, alternate processing sites provide processing capability if the primary processing site is not available. Geographically distributed architectures that support contingency requirements may be considered alternate storage sites. Items covered by alternate storage site agreements include environmental conditions at the alternate sites, access rules for systems and facilities, physical and environmental protection requirements, and coordination of delivery and retrieval of backup media. Alternate storage sites reflect the requirements in contingency plans so that organizations can maintain essential mission and business functions despite compromise, failure, or disruption in organizational systems.

Related Controls: CP-2, CP-7, CP-8, CP-9, CP-10, MP-4, MP-5, PE-3, SC-36, SI-13.

3.18.07e Configure the alternate storage site to achieve system recovery (s) that meets the RTO and RPO

DISCUSSION
Organizations establish recovery time and recovery point objectives as part of contingency planning. Configuration of the alternate storage site includes physical facilities and the systems supporting recovery operations that ensure accessibility and correct execution.

Related Controls: None.

3.18.08e Establish alternate processing site(s) to facilitate the processing of information and data in a manner that meets the RTO and RPO of the system(s)

DISCUSSION
Alternate processing sites are geographically distinct from primary processing sites and provide processing capability if the primary processing site is not available. The alternate processing capability may be addressed using a physical processing site or other alternatives, such as failover to a cloud-based service provider or other internally or externally provided processing service. Geographically distributed architectures that support contingency requirements may also be considered alternate processing sites. Controls that are covered by alternate processing site agreements include the environmental conditions at alternate sites,

access rules, physical and environmental protection requirements, and the coordination for the transfer and assignment of personnel. Requirements are allocated to alternate processing sites that reflect the requirements in contingency plans to maintain essential mission and business functions despite disruption, compromise, or failure in organizational systems.

Related Controls: CP-2, CP-6, CP-8, CP-9, CP-10, MA-6, PE-3, PE-11, PE-12, PE-17, SC-36, SI-13.

3.18.09e Establish alternate telecommunication service capabilities that meet the voice and data requirements of the organization and its systems

DISCUSSION

Telecommunications services (for data and voice) for primary and alternate processing and storage sites are included in the scope of this control. Alternate telecommunications services reflect the continuity requirements in contingency plans to maintain essential mission and business functions despite the loss of primary telecommunications services. Organizations may specify different time periods for primary or alternate sites. Alternate telecommunications services include additional organizational or commercial ground-based circuits or lines, network-based approaches to telecommunications, or the use of satellites. Organizations consider factors such as availability, quality of service, and access when entering into alternate telecommunications agreements.

Related Controls: CP-2, CP-6, CP-7, CP-11, SC-7.

3.18.10e Test the capability and reliability of systems/components to retrieve information/media to meet the RTO and RTO

DISCUSSION

Organizations need assurance that backup information can be reliably retrieved. Reliability pertains to the systems and system components where the backup information is stored, the operations used to retrieve the information, and the integrity of the information being retrieved. Independent and specialized tests can be used for each of the aspects of reliability. For example, decrypting and transporting (or transmitting) a random sample of backup files from the alternate storage or backup site and comparing the information to the same information at the primary processing site can provide such assurance.

Related Controls: CP-4.

3.18.11e Provide for the recovery and reconstitution of the system(s) to a known state within the RTO and RPO objective timeframes

DISCUSSION

Recovery is executing contingency plan activities to restore organizational mission and business functions. Reconstitution takes place following recovery and includes activities for returning systems to fully operational states. Recovery and reconstitution operations reflect mission and business priorities; recovery point, recovery time, and reconstitution objectives; and organizational metrics consistent with contingency plan requirements. Reconstitution includes the deactivation of interim system capabilities that may have been needed during recovery operations. Reconstitution also includes assessments of fully restored system capabilities, reestablishment of continuous monitoring activities, system reauthorization (if required), and activities to prepare the system and organization for future disruptions, breaches, compromises, or failures. Recovery and reconstitution capabilities can include automated mechanisms and manual procedures. Organizations establish recovery time and recovery point objectives as part of contingency planning.

Related Controls: CP-2, CP-4, CP-6, CP-7, CP-9, IR-4, SA-8, SC-24, SI-13.