SP 800-171 Revision 1 Excerpt:

Specific Changes to the Security Requirements in SP 800-171

December 20, 2016

The following provides the specific changes to the security requirements in NIST SP 800-171. If there are any discrepancies between this excerpt and the final publication posted on the NIST web site, the final publication is the authoritative source.

3.1 ACCESS CONTROL

Basic Security Requirements:

3.1.1 Limit ~~information~~ system access to authorized users, processes acting on behalf of authorized users, or devices (including other ~~information~~ systems).

3.1.2 Limit ~~information~~ system access to the types of transactions and functions that authorized users are permitted to execute.

Derived Security Requirements:

3.1.3 Control the flow of CUI in accordance with approved authorizations.

3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.

3.1.6 Use non-privileged accounts or roles when accessing nonsecurity functions.

3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.

3.1.8 Limit unsuccessful logon attempts.

3.1.9 Provide privacy and security notices consistent with applicable CUI rules.

3.1.10 Use session lock with pattern-hiding displays to prevent access and ~~/~~viewing of data after period of inactivity.

3.1.11 Terminate (automatically) a user session after a defined condition.

3.1.12 Monitor and control remote access sessions.

3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

3.1.14 Route remote access via managed access control points.

3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.

3.1.16 Authorize wireless access prior to allowing such connections.

3.1.17 Protect wireless access using authentication and encryption.

3.1.18 Control connection of mobile devices.

3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.[21]

3.1.20 Verify and control/limit connections to and use of external ~~information~~ systems.

3.1.21 Limit use of organizational portable storage devices on external ~~information~~ systems.

3.1.22 Control CUI~~information~~ posted or processed on publicly accessible ~~information~~ systems.

---

[21] Mobile devices and mobile computing platforms include, for example, smartphones, tablets, E-readers, and notebook computers.

3.2 AWARENESS AND TRAINING

Basic Security Requirements:

3.2.1 Ensure that managers, systems administrators, and users of organizational ~~information~~ systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those ~~organizational information~~ systems.

3.2.2 Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Derived Security Requirements:

3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.

3.3 AUDIT AND ACCOUNTABILITY

Basic Security Requirements:

3.3.1 Create, protect, and retain ~~information~~ system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate ~~information~~ system activity.

3.3.2 Ensure that the actions of individual ~~information~~ system users can be uniquely traced to those users so they can be held accountable for their actions.

Derived Security Requirements:

3.3.3 Review and update audited events.

3.3.4 Alert in the event of an audit process failure.

3.3.5 Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.

3.3.6 Provide audit reduction and report generation to support on-demand analysis and reporting.

3.3.7 Provide a ~~an information~~ system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

3.3.8 Protect audit information and audit tools from unauthorized access, modification, and deletion.

3.3.9 Limit management of audit functionality to a subset of privileged users.

3.4 CONFIGURATION MANAGEMENT

Basic Security Requirements:

3.4.1 Establish and maintain baseline configurations and inventories of organizational ~~information~~ systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational ~~information~~ systems.

Derived Security Requirements:

3.4.3 Track, review, approve/disapprove, and audit changes to organizational ~~information~~ systems.

3.4.4 Analyze the security impact of changes prior to implementation.

3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational ~~the information~~ systems.

3.4.6 Employ the principle of least functionality by configuring organizational ~~the information~~ systems to provide only essential capabilities.

3.4.7 Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.

3.4.8 Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

3.4.9 Control and monitor user-installed software.

3.5 IDENTIFICATION AND AUTHENTICATION

Basic Security Requirements:

3.5.1 Identify ~~information~~ system users, processes acting on behalf of users, or devices.

3.5.2 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational ~~information~~ systems.

Derived Security Requirements:

3.5.3 Use multifactor authentication[22] for local and network access[23] to privileged accounts and for network access to non-privileged accounts.

3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

3.5.5 Prevent reuse of identifiers for a defined period.

3.5.6 Disable identifiers after a defined period of inactivity.

3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created.

3.5.8 Prohibit password reuse for a specified number of generations.

3.5.9 Allow temporary password use for system logons with an immediate change to a permanent password.

3.5.10 Store and transmit only cryptographically-protected~~encrypted representation of~~ passwords.

3.5.11 Obscure feedback of authentication information.

3.6 INCIDENT RESPONSE

Basic Security Requirements:

3.6.1 Establish an operational incident-handling capability for organizational ~~information~~ systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.

---

[22] *Multifactor authentication* requires two or more different factors to achieve authentication. The factors~~Factors~~ include: ~~(i)~~ something you know (e.g., password/PIN); ~~(ii)~~ something you have (e.g., cryptographic identification device, token); or ~~(iii)~~ something you are (e.g., biometric). The requirement for multifactor authentication should not be interpreted as requiring federal Personal Identity Verification (PIV) card or Department of Defense Common Access Card (CAC)-like solutions. A variety of multifactor solutions (including those with replay resistance) using tokens and biometrics are commercially available. Such solutions may employ hard tokens (e.g., smartcards, key fobs, or dongles) or soft tokens to store user credentials.

[23] *Local access* is any access to a ~~an information~~ system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network. *Network access* is any access to a ~~an information~~ system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).

3.6.2 Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.

Derived Security Requirements:

3.6.3 Test the organizational incident response capability.

3.7 MAINTENANCE

Basic Security Requirements:

3.7.1 Perform maintenance on organizational ~~information~~ systems.[24]

3.7.2 Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct ~~information~~ system maintenance.

Derived Security Requirements:

3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.

3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational ~~the information~~ systems.

3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.

3.8 MEDIA PROTECTION

Basic Security Requirements:

3.8.1 Protect (i.e., physically control and securely store) ~~information~~ system media containing CUI, both paper and digital.

3.8.2 Limit access to CUI on ~~information~~ system media to authorized users.

3.8.3 Sanitize or destroy ~~information~~ system media containing CUI before disposal or release for reuse.

Derived Security Requirements:

3.8.4 Mark media with necessary CUI markings and distribution limitations.[25]

3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

3.8.7 Control the use of removable media on ~~information~~ system components.

3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner.

3.8.9 Protect the confidentiality of backup CUI at storage locations.

---

[24] In general, system maintenance requirements tend to support the security objective of *availability*. However, improper system maintenance or a failure to perform maintenance can result in the unauthorized disclosure of CUI, thus compromising *confidentiality* of that information.

[25] The implementation of this requirement is per marking guidance in the 32 CFR, Part 2002, and ~~contingent on the finalization of the proposed CUI federal regulation and marking guidance in~~ the CUI Registry.

3.9 PERSONNEL SECURITY

Basic Security Requirements:

3.9.1 Screen individuals prior to authorizing access to organizational ~~information~~ systems containing CUI.

3.9.2 Ensure that CUI and organizational ~~information~~ systems containing CUI are protected during and after personnel actions such as terminations and transfers.

Derived Security Requirements: None.

3.10 PHYSICAL PROTECTION

Basic Security Requirements:

3.10.1 Limit physical access to organizational ~~information~~ systems, equipment, and the respective operating environments to authorized individuals.

3.10.2 Protect and monitor the physical facility and support infrastructure for organizational ~~those information~~ systems.

Derived Security Requirements:

3.10.3 Escort visitors and monitor visitor activity.

3.10.4 Maintain audit logs of physical access.

3.10.5 Control and manage physical access devices.

3.10.6 Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).

3.11 RISK ASSESSMENT

Basic Security Requirements:

3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational ~~information~~ systems and the associated processing, storage, or transmission of CUI.

Derived Security Requirements:

3.11.2 Scan for vulnerabilities in organizational ~~the information~~ systems and applications periodically and when new vulnerabilities affecting those ~~the~~ systems and applications are identified.

3.11.3 Remediate vulnerabilities in accordance with assessments of risk.

3.12 SECURITY ASSESSMENT

Basic Security Requirements:

3.12.1 Periodically assess the security controls in organizational ~~information~~ systems to determine if the controls are effective in their application.

3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational ~~information~~ systems.

3.12.3 Monitor ~~information system~~ security controls on an ongoing basis to ensure the continued effectiveness of the controls.

3.12.4 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. [26]

Derived Security Requirements: None.

3.13 SYSTEM AND COMMUNICATIONS PROTECTION

Basic Security Requirements:

3.13.1 Monitor, control, and protect ~~organizational~~ communications (i.e., information transmitted or received by organizational ~~information~~ systems) at the external boundaries and key internal boundaries of ~~the~~ organizational ~~information~~ systems.

3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational ~~information~~ systems.

Derived Security Requirements:

3.13.3 Separate user functionality from ~~information~~ system management functionality.

3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.

3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational ~~the information~~ systems and communicating via some other connection to resources in external networks.

3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational ~~the information~~ systems.

3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

3.13.12 Prohibit remote activation [27] of collaborative computing devices and provide indication of devices in use to users present at the device.

3.13.13 Control and monitor the use of mobile code.

3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

3.13.15 Protect the authenticity of communications sessions.

3.13.16 Protect the confidentiality of CUI at rest.

---

[26] There is no prescribed format or specified level of detail for *system security plans*. However, organizations must ensure that the required information in 3.12.4 is appropriately conveyed in those plans.

[27] Dedicated video conferencing systems, which rely on one of the participants calling or connecting to the other party to activate the video conference, are excluded.

3.14 SYSTEM AND INFORMATION INTEGRITY

Basic Security Requirements:

3.14.1 Identify, report, and correct information and ~~information~~ system flaws in a timely manner.

3.14.2 Provide protection from malicious code at appropriate locations within organizational ~~information~~ systems.

3.14.3 Monitor ~~information~~ system security alerts and advisories and take appropriate actions in response.

Derived Security Requirements:

3.14.4 Update malicious code protection mechanisms when new releases are available.

3.14.5 Perform periodic scans of organizational ~~the information~~ systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

3.14.6 Monitor organizational ~~the information~~ systems including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

3.14.7 Identify unauthorized use of organizational ~~the information~~ systems.