NIST Special Publication 800
NIST SP 800-171r3

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Ron Ross
Victoria Pillitteri

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r3

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

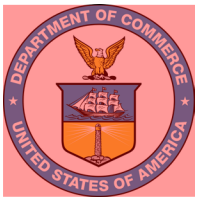
NIST Special Publication 800
NIST SP 800-171r3

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Ron Ross
Victoria Pillitteri
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r3

May 2024



U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Authority
This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History
Approved by the NIST Editorial Review Board on 2024-04-23
Supersedes NIST Special Publication 800-171r2 (February 2020; Includes updates as of 01-28-2021)
https://doi.org/10.6028/NIST.SP.800-171r2

How to Cite this NIST Technical Series Publication:
Ross R, Pillitteri V (2024) Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-171r3. https://doi.org/10.6028/NIST.SP.800-171r3

Author ORCID iDs
Ron Ross: 0000-0002-1099-9757
Victoria Pillitteri: 0000-0002-7446-7506

Submit Comments

800-171comments@list.nist.gov
National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

Additional Information

Additional information about this publication is available at https://csrc.nist.gov/pubs/sp/800/171/r3/final, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

The protection of Controlled Unclassified Information (CUI) is of paramount importance to federal agencies and can directly impact the ability of the Federal Government to successfully conduct its essential missions and functions. This publication provides federal agencies with recommended security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems and organizations. The requirements apply to components of nonfederal systems that process, store, or transmit CUI *or* that provide protection for such components. The security requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations. This publication can be used in conjunction with its companion publication, NIST Special Publication 800-171A, which provides a comprehensive set of procedures to assess the security requirements.

Keywords

Controlled Unclassified Information; Executive Order 13556; FIPS Publication 199; FIPS Publication 200; FISMA; NIST Special Publication 800-53; nonfederal organizations; nonfederal systems; organization-defined parameter; security assessment; security control; security requirement.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Audience

This publication serves a diverse group of individuals and organizations in the public and private sectors, including:

- Federal agencies responsible for managing and protecting CUI
- Nonfederal organizations responsible for protecting CUI
- Individuals with system development life cycle responsibilities (e.g., program managers, mission/business owners, information owners/stewards, system designers and developers, system/security engineers, systems integrators)
- Individuals with acquisition or procurement responsibilities (e.g., contracting officers)
- Individuals with system, security, or risk management and oversight responsibilities (e.g., authorizing officials, chief information officers, chief information security officers, system owners, information security managers)
- Individuals with security assessment and monitoring responsibilities (e.g., auditors, system evaluators, assessors, analysts, independent verifiers and validators)

The above roles and responsibilities can be viewed from two perspectives:

- *Federal perspective*: The entity establishing and conveying the security requirements in contractual vehicles or other types of agreements
- *Nonfederal perspective*: The entity responding to and complying with the security requirements set forth in contracts or agreements

Patent Disclosure Notice

NOTICE: ITL has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Table of Contents

List of Tables

Acknowledgments

The authors gratefully acknowledge and appreciate the significant contributions from individuals and organizations in the public and private sectors whose constructive comments improved the overall quality, thoroughness, and usefulness of this publication. The authors also wish to thank the NIST technical editing and production staff – Jim Foti, Jeff Brewer, Eduardo Takamura, Isabel Van Wyk, Cristina Ritfeld, Derek Sappington, and Carolyn Schmidt – for their outstanding support in preparing this document for publication. Finally, a special note of thanks goes out to Kelley Dempsey for the initial research and development of the content used in the prototype CUI overlay.

Historical Contributions

The authors also wish to acknowledge the following organizations and individuals for their historic contributions to this publication:

- *Organizations:* National Archives and Records Administration, Department of Defense
- *Individuals:* Carol Bales, Matthew Barrett, Jon Boyens, Devin Casey, Christian Enloe, Gary Guissanie, Peggy Himes, Robert Glenn, Elizabeth Lennon, Vicki Michetti, Dorian Pappas, Karen Quigg, Mark Riddle, Matthew Scholl, Mary Thomas, Murugiah Souppaya, Patricia Toth, and Patrick Viscuso

1. Introduction

Executive Order (EO) 13556 [1] established a government-wide program to standardize the way the executive branch handles Controlled Unclassified Information (CUI).[1] EO 13556 required that the CUI program emphasize openness, transparency, and uniformity of government-wide practices and that the program implementation take place in a manner consistent with Office of Management and Budget (OMB) policies and National Institute of Standards and Technology (NIST) standards and guidelines. As the CUI program Executive Agent, the National Archives and Records Administration (NARA) provides information, guidance, policy, and requirements on handling CUI [4]. This includes approved CUI categories and descriptions, the basis for safeguarding and dissemination controls, and procedures for the use of CUI.[2] The CUI federal regulation [5] provides guidance to federal agencies on the designation, safeguarding, marking, dissemination, decontrolling, and disposition of CUI; establishes self-inspection and oversight requirements; and delineates other facets of the program.

The CUI regulation requires federal agencies that use federal information systems[3] to process, store, or transmit CUI to comply with NIST standards and guidelines. The responsibility of federal agencies to protect CUI does not change when such information is shared with nonfederal organizations.[4] Therefore, a similar level of protection is needed when CUI is processed, stored, or transmitted by nonfederal organizations using nonfederal systems.[5] To maintain a consistent level of protection, the security requirements for safeguarding CUI in nonfederal systems and organizations must comply with Federal Information Processing Standards (FIPS 199) publication [6] and FIPS 200 [7]. The requirements are derived from the controls in NIST Special Publication (SP) 800-53 [8].

1.1. Purpose and Applicability

This publication provides federal agencies with recommended security requirements[6] for protecting the *confidentiality* of CUI[7] when such information is resident in nonfederal systems and organizations and where there are no specific safeguarding requirements prescribed by the authorizing law, regulation, or government-wide policy for the CUI category listed in the CUI

[1] CUI is any information that a law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under EO 13526 [2], any predecessor or successor order, or the Atomic Energy Act [3] as amended.

[2] Procedures for the use of CUI include marking, safeguarding, transporting, disseminating, reusing, and disposing of the information.

[3] A *federal information system* is a system that is used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. The term *system* is used in this publication to represent people, processes, and technologies involved in the processing, storage, or transmission of CUI. Systems can include operational technology (OT), information technology (IT), Internet of Things (IoT) devices, Industrial IoT (IIoT) devices, specialized systems, cyber-physical systems, embedded systems, and sensors.

[4] A *nonfederal organization* is any entity that owns, operates, or maintains a nonfederal system.

[5] A *nonfederal system* is any system that does not meet the criteria for a federal information system.

[6] The term *security requirement* refers to the protection needs for a system or organization. Security requirements may be derived from laws, Executive Orders, directives, regulations, policies, standards, mission and business needs, or risk assessments.

[7] In accordance with EO 13526 [2] and 32 CFR 2002 [5], the scope of CUI protection is primarily focused on *confidentiality*. However, the security objectives of confidentiality and integrity are closely related since many of the underlying security mechanisms support both objectives. Therefore, the security requirements in this publication address the protection of CUI from unauthorized disclosure and modification.

registry [4]. The requirements do not apply to nonfederal organizations that are collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency.[8]

The security requirements in this publication are *only* applicable to components of nonfederal systems that process, store, or transmit CUI *or* that provide protection for such components.[9] The requirements are intended for use by federal agencies in contractual vehicles or other agreements that are established between those agencies and nonfederal organizations.

Appropriately scoping requirements is an important factor in determining protection-related investment decisions and managing security risks for nonfederal organizations. If nonfederal organizations designate system components for the processing, storage, or transmission of CUI, those organizations may limit the scope of the security requirements by isolating the system components in a separate security domain. Isolation can be achieved by applying architectural and design concepts (e.g., implementing subnetworks with firewalls or other boundary protection devices and using information flow control mechanisms). Security domains may employ physical separation, logical separation, or a combination of both. This approach can provide adequate security for CUI and avoid increasing the organization's security posture beyond what it requires for protecting its missions, operations, and assets.

1.2. Organization of This Publication

The remainder of this special publication is organized as follows:

- Section 2 describes the assumptions and methodology used to develop the security requirements for protecting the confidentiality of CUI, the format of the requirements, and the tailoring criteria applied to the NIST guidelines to obtain the requirements.
- Section 3 lists the security requirements for protecting the confidentiality of CUI in nonfederal systems and organizations.

The following sections provide additional information to support the protection of CUI:

- References
- Appendix A: Acronyms
- Appendix B: Glossary
- Appendix C: Tailoring Criteria
- Appendix D: Organization-Defined Parameters
- Appendix E: Change Log

[8] Nonfederal organizations that collect or maintain information on behalf of a federal agency or that use or operate a system on behalf of an agency must comply with the requirements in FISMA [9].

[9] System *components* include workstations, servers, notebook computers, smartphones, tablets, input and output devices, network components, operating systems, virtual machines, database management systems, and applications.

2. The Fundamentals

This section describes the assumptions and methodology used to develop the requirements to protect the confidentiality of CUI in nonfederal systems and organizations. It also includes the tailoring[10] criteria applied to the controls in SP 800-53 [8].

2.1. Security Requirement Assumptions

The security requirements in this publication are based on the following assumptions:

- Federal information designated as CUI has the same value, whether such information resides in a federal or nonfederal system or organization.
- Statutory and regulatory requirements for the protection of CUI are consistent in federal and nonfederal systems and organizations.
- Safeguards implemented to protect CUI are consistent in federal and nonfederal systems and organizations.
- The confidentiality impact value for CUI is no less than *moderate*.[11]
- Nonfederal organizations can directly implement a variety of potential security solutions or use external service providers to satisfy security requirements.

2.2. Security Requirement Development Methodology

Starting with the SP 800-53 controls in the SP 800-53B [12] moderate baseline, the controls are *tailored* to eliminate selected controls or parts of controls that are:

- Primarily the responsibility of the Federal Government,
- Not directly related to protecting the confidentiality of CUI,
- Adequately addressed by other related controls,[12] or
- Not applicable.

SP 800-171 security requirements represent a subset of the controls that are necessary to protect the confidentiality of CUI. The security requirements are organized into 17 families, as illustrated in Table 1. Each family contains the requirements related to the general security topic of the family. Certain families from SP 800-53 are not included due to the tailoring criteria. For example, the PII Processing and Transparency (PT) family is not included because personally identifiable information (PII) is a category of CUI, and therefore, no additional requirements are

[10] *Tailoring* is the process by which control baselines are modified to achieve certain organizational goals and objectives [13].

[11] In accordance with 32 CFR 2002 [5], CUI is categorized at no less than the FIPS 199 [6] moderate confidentiality impact value. However, when federal law, regulation, or government-wide policy establishing the control of CUI specifies controls that differ from those of the moderate control baseline, then the applicable law, regulation, or government-wide policy is followed.

[12] "Adequately addressed by other related controls" means that the protection capability offered by the control is provided by another control in the same or different control family. Using this tailoring option helps to eliminate potential redundancy in requirements without affecting the protection of CUI in nonfederal systems and organizations.

specified for confidentiality protection. The Program Management (PM) family is not included because it is not associated with any control baseline. Finally, the Contingency Planning (CP) family is not included because it addresses availability.[13]

Table 1. Security Requirement Families

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

Organization-defined parameters (ODPs) are included in certain security requirements. ODPs provide flexibility through the use of *assignment* and *selection* operations to allow federal agencies and nonfederal organizations to specify values for the designated parameters in the requirements.[14] Assignment and selection operations provide the capability to customize the security requirements based on specific protection needs. The determination of ODP values can be guided and informed by laws, Executive Orders, directives, regulations, policies, standards, guidance, or mission and business needs. Once specified, the values for the organization-defined parameters become part of the requirement.

ORGANIZATION-DEFINED PARAMETERS

Organization-defined parameters are an important part of a security requirement specification. ODPs provide both the flexibility and specificity needed by organizations to clearly define their CUI security requirements, given the diverse nature of their missions, business functions, operational environments, and risk tolerance. In addition, ODPs support consistent security assessments in determining whether specified security requirements have been satisfied. If a federal agency or a consortium of agencies do not specify a particular value or range of values for an ODP, nonfederal organizations must assign the value or values to complete the security requirement.

A discussion section is included with each requirement. It is derived from the control discussion sections in SP 800-53 and provides additional information to facilitate the implementation and assessment of the requirements. The discussion section is informative, not normative. It is not intended to extend the scope of a requirement or influence the solutions that organizations may use to satisfy a requirement. The use of examples is notional, not exhaustive, and does not reflect the potential options available to organizations. A *references* section provides the source

[13] CP-09 and CP-09(08) are included by exception to ensure the confidentiality of backup information is projected.

[14] NIST does not establish or assign values for ODPs. If ODP values for selected security requirements are not formally established or assigned by a federal agency or a consortium of federal agencies, nonfederal organizations must assign those values to complete the requirements.

controls[15] from SP 800-53 and a list of NIST Special Publications with additional information on the topic described in the security requirement. The structure and content of a typical security requirement is provided in the example below.

03.13.11 Cryptographic Protection

Implement the following types of cryptography when used to protect the confidentiality of CUI: [*Assignment: organization-defined types of cryptography*].

DISCUSSION

Cryptography is implemented in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines. FIPS-validated cryptography is recommended for the protection of CUI.

REFERENCES

Source Control: SC-13

Supporting Publications: FIPS 140-3 [38]

The term *organization* is used in many security requirements, and its meaning depends on context. For example, in a security requirement with an ODP, an organization can refer to either the federal agency or the nonfederal organization establishing the parameter values for the requirement.

Appendix C describes the security control tailoring criteria used to develop the security requirements and the results of the tailoring process. The appendix provides a list of controls from SP 800-53 that support the requirements and the controls that have been eliminated from the moderate baseline in accordance with the tailoring criteria.

ASSESSING SECURITY REQUIREMENTS

SP 800-171A [84] provides a set of procedures to assess the security requirements described in this publication. The assessment procedures are based on the procedures described in SP 800-53A [57].

[15] With few exceptions, the security controls in SP 800-53 are policy-, technology-, and sector-neutral, meaning that the controls focus on the fundamental measures necessary to protect information across the information life cycle.

3. The Security Requirements

This section describes 17 families of security requirements for protecting the confidentiality of CUI in nonfederal systems and organizations. When used in the context of the requirements in Sec. 3, the term *system* is defined to be nonfederal systems or system components that process, store, or transmit CUI or that provide protection for such systems or components. Not all security requirements mention CUI explicitly. However, the requirements are included because they directly affect the protection of CUI during processing, while in storage, and when in transmission between different locations.

Some systems, including specialized systems (e.g., industrial/process control systems, medical devices, computer numerical control machines), may have limitations on the application of certain security requirements. To accommodate such issues, the system security plan — as reflected in requirement 03.15.02 — is used to describe any *enduring exceptions* to the security requirements. Individual, isolated, or temporary deficiencies are managed though plans of action and milestones, as reflected in requirement 03.12.02.

SCOPE AND APPLICABILITY OF SECURITY REQUIREMENTS

The security requirements in this section are only applicable to components of nonfederal systems that process, store, or transmit CUI *or* that provide protection for such components.

3.1. Access Control

03.01.01 Account Management

a. Define the types of system accounts allowed and prohibited.

b. Create, enable, modify, disable, and remove system accounts in accordance with policy, procedures, prerequisites, and criteria.

c. Specify:

   1. Authorized users of the system,
   2. Group and role membership, and
   3. Access authorizations (i.e., privileges) for each account.

d. Authorize access to the system based on:

   1. A valid access authorization and
   2. Intended system usage.

e. Monitor the use of system accounts.

f. Disable system accounts when:

1. The accounts have expired,
2. The accounts have been inactive for [*Assignment: organization-defined time period*],
3. The accounts are no longer associated with a user or individual,
4. The accounts are in violation of organizational policy, or
5. Significant risks associated with individuals are discovered.

g. Notify account managers and designated personnel or roles within:

1. [*Assignment: organization-defined time period*] when accounts are no longer required.
2. [*Assignment: organization-defined time period*] when users are terminated or transferred.
3. [*Assignment: organization-defined time period*] when system usage or the need-to-know changes for an individual.

h. Require that users log out of the system after [*Assignment: organization-defined time period*] of expected inactivity or when [*Assignment: organization-defined circumstances*].

DISCUSSION

This requirement focuses on account management for systems and applications. The definition and enforcement of access authorizations other than those determined by account type (e.g., privileged access, non-privileged access) are addressed in 03.01.02. System account types include individual, group, temporary, system, guest, anonymous, emergency, developer, and service. Users who require administrative privileges on system accounts receive additional scrutiny by personnel responsible for approving such accounts and privileged access. Types of accounts that organizations may prohibit due to increased risk include group, emergency, guest, anonymous, and temporary.

Organizations may choose to define access privileges or other attributes by account, type of account, or a combination of both. Other attributes required for authorizing access include restrictions on the time of day, day of the week, and point of origin. When defining other system account attributes, organizations consider system requirements (e.g., system upgrades, scheduled maintenance) and mission and business requirements (e.g., time zone differences, remote access to facilitate travel requirements).

Users who pose a significant security risk include individuals for whom reliable evidence indicates either the intention to use authorized access to the system to cause harm or that adversaries will cause harm through them. Close coordination

among mission and business owners, system administrators, human resource managers, and legal staff is essential when disabling system accounts for high-risk individuals. Time periods for the notification of organizational personnel or roles may vary.

Inactivity logout is behavior- or policy-based and requires users to take physical action to log out when they are expecting inactivity longer than the defined period. Automatic enforcement of inactivity logout is addressed by 03.01.10.

REFERENCES

Source Controls: AC-02, AC-02(03), AC-02(05), AC-02(13)

Supporting Publications: SP 800-46 [14], SP 800-57-1 [15], SP 800-57-2 [16], SP 800-57-3 [17], SP 800-77 [18], SP 800-113 [19], SP 800-114 [20], SP 800-121 [21], SP 800-162 [22], SP 800-178 [23], SP 800-192 [24], IR 7874 [25], IR 7966 [26]

03.01.02 Access Enforcement

Enforce approved authorizations for logical access to CUI and system resources in accordance with applicable access control policies.

DISCUSSION

Access control policies control access between active entities or subjects (i.e., users or system processes acting on behalf of users) and passive entities or objects (i.e., devices, files, records, domains) in organizational systems. Types of system access include remote access and access to systems that communicate through external networks, such as the internet. Access enforcement mechanisms can also be employed at the application and service levels to provide increased protection for CUI. This recognizes that the system can host many applications and services in support of mission and business functions. Access control policies are defined in 03.15.01.

REFERENCES

Source Control: AC-03

Supporting Publications: SP 800-46 [14], SP 800-57-1 [15], SP 800-57-2 [16], SP 800-57-3 [17], SP 800-77 [18], SP 800-113 [19], SP 800-114 [20], SP 800-121 [21], SP 800-162 [22], SP 800-178 [23], SP 800-192 [24], IR 7874 [25], IR 7966 [26]

03.01.03 Information Flow Enforcement

Enforce approved authorizations for controlling the flow of CUI within the system and between connected systems.

DISCUSSION

Information flow control regulates where CUI can transit within a system and between systems (in contrast to who is allowed to access the information) and without regard to subsequent accesses to that information. Flow control restrictions include keeping CUI from being transmitted in the clear to the internet, blocking external communications traffic that claims to be sourced from within the organization, restricting requests to the internet that are not from the internal web proxy server, and limiting CUI transfers between organizations based on data structures and content.

Transferring CUI between organizations may require an agreement that specifies how the information flow is enforced (see 03.12.05). Transferring CUI between systems that represent different security domains with different security policies introduces the risk that such transfers violate one or more domain security policies. In such situations, information owners or stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies. Enforcement includes prohibiting CUI transfers between interconnected systems (i.e., allowing information access only), employing hardware mechanisms to enforce one-way information flows, and implementing trustworthy regrading mechanisms to reassign security attributes and security labels.

Organizations commonly use information flow control policies and enforcement mechanisms to control the flow of CUI between designated sources and destinations (e.g., networks, individuals, and devices) within systems and between interconnected systems. Flow control is based on characteristics of the information or the information path. Enforcement occurs in boundary protection devices (e.g., encrypted tunnels, routers, gateways, and firewalls) that use rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or provide a message-filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering and inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement.

REFERENCES

Source Control: AC-04

Supporting Publications: SP 800-160-1 [11], SP 800-162 [22], SP 800-178 [23]

03.01.04 Separation of Duties

a. Identify the duties of individuals requiring separation.

b. Define system access authorizations to support separation of duties.

DISCUSSION

Separation of duties addresses the potential for abuse of authorized privileges and reduces the risk of malevolent activity without collusion. Separation of duties includes dividing mission functions and support functions among different individuals or roles, conducting system support functions with different individuals or roles (e.g., quality assurance, configuration management, network security, system management, assessments, and programming), and ensuring that personnel who administer access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of their systems and system components when developing policies on separation of duties. This requirement is enforced by 03.01.02.

REFERENCES

Source Control: AC-05

Supporting Publications: SP 800-162 [22], SP 800-178 [23]

03.01.05 Least Privilege

a. Allow only authorized system access for users (or processes acting on behalf of users) that is necessary to accomplish assigned organizational tasks.

b. Authorize access to [*Assignment: organization-defined security functions*] and [*Assignment: organization-defined security-relevant information*].

c. Review the privileges assigned to roles or classes of users [*Assignment: organization-defined frequency*] to validate the need for such privileges.

d. Reassign or remove privileges, as necessary.

DISCUSSION

Organizations employ the principle of least privilege for specific duties and authorized access for users and system processes. Least privilege is applied to the development, implementation, and operation of the system. Organizations consider creating additional processes, roles, and system accounts to achieve least privilege. Security functions include establishing system accounts and assigning privileges, installing software, configuring access authorizations, configuring settings for events to be audited, establishing vulnerability scanning parameters, establishing intrusion detection parameters, and managing audit information. Security-relevant information includes threat and vulnerability information, filtering rules for routers or firewalls, configuration parameters for security services, security architecture, cryptographic key management information, access control lists, and audit information.

REFERENCES

Source Controls: AC-06, AC-06(01), AC-06(07), AU-09(04)

Supporting Publications: None

03.01.06 Least Privilege – Privileged Accounts

a. Restrict privileged accounts on the system to [*Assignment: organization-defined personnel or roles*].

b. Require that users (or roles) with privileged accounts use non-privileged accounts when accessing non-security functions or non-security information.

DISCUSSION

Privileged accounts refer to accounts that are granted elevated privileges to access resources (including security functions or security-relevant information) that are otherwise restricted for non-privileged accounts. These accounts are typically described as system administrator or super user accounts. For example, a privileged account is often required in order to perform privileged functions such as executing commands that could modify system behavior. Restricting privileged accounts to specific personnel or roles ensures that only those authorized users can access and manipulate security functions or security-relevant information. Requiring the use of non-privileged accounts when such access is not needed can limit unauthorized access to and manipulation of security functions or security-relevant information.

REFERENCES

Source Controls: AC-06(02), AC-06(05)

Supporting Publications: None

03.01.07 Least Privilege – Privileged Functions

a. Prevent non-privileged users from executing privileged functions.

b. Log the execution of privileged functions.

DISCUSSION

Privileged functions include establishing system accounts, performing system integrity checks, conducting patching operations, changing system configuration settings, or administering cryptographic key management activities. Non-privileged users do not possess the authorizations to execute privileged functions. Bypassing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users. This requirement represents a condition achieved by the definition of authorized privileges in 03.01.01 and privilege enforcement in 03.01.02.

The misuse of privileged functions — whether intentionally or unintentionally by authorized users or by unauthorized external entities that have compromised system accounts — is a serious and ongoing concern that can have significant adverse impacts on organizations. Logging the use of privileged functions is one way to detect such misuse and mitigate risks from advanced persistent threats and insider threats.

REFERENCES

Source Controls: AC-06(09), AC-06(10)

Supporting Publications: None

03.01.08 Unsuccessful Logon Attempts

a. Enforce a limit of [*Assignment: organization-defined number*] consecutive invalid logon attempts by a user during a [*Assignment: organization-defined time period*].

b. Automatically [*Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt; notify system administrator; take other action*] when the maximum number of unsuccessful attempts is exceeded.

DISCUSSION

Due to the potential for denial of service, automatic system lockouts are in most cases, temporary and automatically release after a predetermined time period established by the organization (i.e., using a delay algorithm). Organizations may employ different delay algorithms for different system components based on the capabilities of the respective components. Responses to unsuccessful system logon attempts may be implemented at the system and application levels.

Organization-defined actions that may be taken include prompting the user to answer a secret question in addition to the username and password, invoking a lockdown mode with limited user capabilities (instead of a full lockout), allowing users to only logon from specified Internet Protocol (IP) addresses, requiring a CAPTCHA to prevent automated attacks, or applying user profiles, such as location, time of day, IP address, device, or Media Access Control (MAC) address.

REFERENCES

Source Control: AC-07

Supporting Publications: SP 800-63-3 [27], SP 800-124 [28]

03.01.09 System Use Notification

Display a system use notification message with privacy and security notices consistent with applicable CUI rules before granting access to the system.

DISCUSSION

System use notifications can be implemented using messages or warning banners. The messages or warning banners are displayed before individuals log in to a system that processes, stores, or transmits CUI. System use notifications are used for access via logon interfaces with human users and are not required when human interfaces do not exist. Organizations consider whether a secondary use notification is needed to access applications or other system resources after the initial network logon. Posters or other printed materials may be used in lieu of an automated system message. This requirement is related to 03.15.03.

REFERENCES

Source Control: AC-08

Supporting Publications: None

03.01.10 Device Lock

a. Prevent access to the system by [*Selection (one or more): initiating a device lock after* [*Assignment: organization-defined time period*] *of inactivity; requiring the user to initiate a device lock before leaving the system unattended*].

b. Retain the device lock until the user reestablishes access using established identification and authentication procedures.

c. Conceal, via the device lock, information previously visible on the display with a publicly viewable image.

DISCUSSION

Device locks are temporary actions taken to prevent access to the system when users depart from the immediate vicinity of the system but do not want to log out due to the temporary nature of their absences. Device locks can be implemented at the operating system level or application level. User-initiated device locking is behavior- or policy-based and requires users to take physical action to initiate the device lock. Device locks are not an acceptable substitute for logging out of the system (e.g., when organizations require users to log out at the end of workdays). Publicly viewable images can include static or dynamic images, such as patterns used with screen savers, solid colors, photographic images, a clock, a battery life indicator, or a blank screen with the caveat that controlled unclassified information is not displayed.

REFERENCES

Source Controls: AC-11, AC-11(01)

Supporting Publications: None

03.01.11 Session Termination

Terminate a user session automatically after [*Assignment: organization-defined conditions or trigger events requiring session disconnect*].

DISCUSSION

This requirement addresses the termination of user-initiated logical sessions in contrast to the termination of network connections that are associated with communications sessions (i.e., disconnecting from the network) in 03.13.09. A logical session is initiated whenever a user (or processes acting on behalf of a user) accesses a system. Logical sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination ends all system processes associated with a user's logical session except those processes that are created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events that require automatic session termination can include organization-defined periods of user inactivity, time-of-day restrictions on system use, and targeted responses to certain types of incidents.

REFERENCES

Source Control: AC-12

Supporting Publications: None

03.01.12 Remote Access

a. Establish usage restrictions, configuration requirements, and connection requirements for each type of allowable remote system access.

b. Authorize each type of remote system access prior to establishing such connections.

c. Route remote access to the system through authorized and managed access control points.

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

DISCUSSION

Remote access is access to systems (or processes acting on behalf of users) that communicate through external networks, such as the internet. Monitoring and controlling remote access methods allows organizations to detect attacks and

ensure compliance with remote access policies. Routing remote access through managed access control points enhances explicit control over such connections and reduces susceptibility to unauthorized access to the system, which could result in the unauthorized disclosure of CUI.

Remote access to the system represents a significant potential vulnerability that can be exploited by adversaries. Restricting the execution of privileged commands and access to security-relevant information via remote access reduces the exposure of the organization and its susceptibility to threats by adversaries. A privileged command is a human-initiated command executed on a system that involves the control, monitoring, or administration of the system, including security functions and security-relevant information. Security-relevant information is information that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data. Privileged commands give individuals the ability to execute sensitive, security-critical, or security-relevant system functions.

REFERENCES

Source Controls: AC-17, AC-17(03), AC-17(04)

Supporting Publications: SP 800-46 [14], SP 800-77 [18], SP 800-113 [19], SP 800-114 [20], SP 800-121 [21], IR 7966 [26]

03.01.13 Withdrawn

Addressed by 03.13.08.

03.01.14 Withdrawn

Incorporated into 03.01.12.

03.01.15 Withdrawn

Incorporated into 03.01.12.

03.01.16 Wireless Access

a. Establish usage restrictions, configuration requirements, and connection requirements for each type of wireless access to the system.

b. Authorize each type of wireless access to the system prior to establishing such connections.

c. Disable, when not intended for use, wireless networking capabilities prior to issuance and deployment.

d. Protect wireless access to the system using authentication and encryption.

DISCUSSION

Wireless networking capabilities represent a significant potential vulnerability that can be exploited by adversaries. Establishing usage restrictions, configuration requirements, and connection requirements for wireless access to the system provides criteria to support access authorization decisions. These restrictions and requirements reduce susceptibility to unauthorized system access through wireless technologies. Wireless networks use authentication protocols that provide credential protection and mutual authentication. Organizations authenticate individuals and devices to protect wireless access to the system. Special attention is given to the variety of devices with potential wireless access to the system, including small form factor mobile devices (e.g., smart phones, tablets, smart watches). Wireless networking capabilities that are embedded within system components represent a potential vulnerability that can be exploited by adversaries. Strong authentication of users and devices, strong encryption, and disabling wireless capabilities that are not needed for essential mission or business functions can reduce susceptibility to threats by adversaries involving wireless technologies.

REFERENCES

Source Controls: AC-18, AC-18(01), AC-18(03)

Supporting Publications: SP 800-94 [29], SP 800-97 [30], SP 800-124 [28]

03.01.17 Withdrawn

Incorporated into 03.01.16.

03.01.18 Access Control for Mobile Devices

a. Establish usage restrictions, configuration requirements, and connection requirements for mobile devices.

b. Authorize the connection of mobile devices to the system.

c. Implement full-device or container-based encryption to protect the confidentiality of CUI on mobile devices.

DISCUSSION

A mobile device is a computing device with a small form factor such that it can be carried by a single individual; is designed to operate without a physical connection; possesses local, non-removable, or removable data storage; and includes a self-contained power source. Mobile device functionality may include on-board sensors that allow the device to capture information, voice communication capabilities, and/or built-in features for synchronizing local data with remote locations. Examples

include smart phones, smart watches, and tablets. Mobile devices are typically associated with a single individual. The processing, storage, and transmission capabilities of mobile devices may be comparable to or a subset of notebook or desktop systems, depending on the nature and intended purpose of the device. Some organizations may consider notebook computers to be mobile devices. The protection and control of mobile devices are behavior- or policy-based and require users to take physical action to protect and control such devices when outside of controlled areas. Controlled areas are spaces for which the organization provides physical or procedural controls to meet the requirements established for protecting CUI.

Due to the large variety of mobile devices with different characteristics and capabilities, organizational restrictions may vary for the different classes or types of such devices. Usage restrictions, configuration requirements, and connection requirements for mobile devices include configuration management, device identification and authentication, implementing mandatory protective software, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting operating system and possibly other software integrity checks, and disabling unnecessary hardware. On mobile devices, secure containers provide software-based data isolation designed to segment enterprise applications and information from personal apps and data. Containers may present multiple user interfaces, one of the most common being a mobile application that acts as a portal to a suite of business productivity apps, such as email, contacts, and calendar. Organizations can employ full-device encryption or container-based encryption to protect the confidentiality of CUI on mobile devices.

REFERENCES

Source Controls: AC-19, AC-19(05)

Supporting Publications: SP 800-46 [14], SP 800-114 [31], SP 800-124 [28]

03.01.19 Withdrawn

Incorporated into 03.01.18.

03.01.20 Use of External Systems

a. Prohibit the use of external systems unless the systems are specifically authorized.

b. Establish the following security requirements to be satisfied on external systems prior to allowing use of or access to those systems by authorized individuals: [*Assignment: organization-defined security requirements*].

c. Permit authorized individuals to use external systems to access the organizational system or to process, store, or transmit CUI only after:

1. Verifying that the security requirements on the external systems as specified in the organization's system security plans have been satisfied and
2. Retaining approved system connection or processing agreements with the organizational entities hosting the external systems.

d. Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems.

DISCUSSION

External systems are systems that are used by but are not part of the organization. These systems include personally owned systems, system components, or devices; privately owned computing and communication devices in commercial or public facilities; systems owned or controlled by nonfederal organizations; and systems managed by contractors. Organizations have the option to prohibit the use of any type of external system or specified types of external systems (e.g., prohibit the use of external systems that are not organizationally owned). Terms and conditions are consistent with the trust relationships established with the entities that own, operate, or maintain external systems and include descriptions of shared responsibilities.

Authorized individuals include organizational personnel, contractors, or other individuals with authorized access to the organizational system and over whom organizations have the authority to impose specific rules of behavior regarding system access. Restrictions that organizations impose on authorized individuals may vary depending on the trust relationships between organizations. Organizations need assurance that external systems satisfy the necessary security requirements so as not to compromise, damage, or harm the system. This requirement is related to 03.16.03.

REFERENCES

Source Controls: AC-20, AC-20(01), AC-20(02)

Supporting Publications: None

03.01.21 Withdrawn

Incorporated into 03.01.20.

03.01.22 Publicly Accessible Content

a. Train authorized individuals to ensure that publicly accessible information does not contain CUI.

b. Review the content on publicly accessible systems for CUI and remove such information, if discovered.

DISCUSSION

In accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidelines, the public is not authorized to have access to nonpublic information, including CUI.

REFERENCES

Source Control: AC-22

Supporting Publications: None

3.2. Awareness and Training

03.02.01 Literacy Training and Awareness

a. Provide security literacy training to system users:
   1. As part of initial training for new users and [*Assignment: organization-defined frequency*] thereafter,
   2. When required by system changes or following [*Assignment: organization-defined events*], and
   3. On recognizing and reporting indicators of insider threat, social engineering, and social mining.

b. Update security literacy training content [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

DISCUSSION

Organizations provide basic and advanced levels of security literacy training to system users (including managers, senior executives, system administrators, and contractors) and measures to test the knowledge level of users. Organizations determine the content of literacy training based on specific organizational requirements, the systems to which personnel have authorized access, and work environments (e.g., telework). The content includes an understanding of the need for security and the actions required of users to maintain security and respond to incidents. The content also addresses the need for operations security and the handling of CUI.

Security awareness techniques include displaying posters, offering supplies inscribed with security reminders, generating email advisories or notices from organizational officials, displaying logon screen messages, and conducting awareness events using podcasts, videos, and webinars. Security literacy training is conducted at a frequency consistent with applicable laws, directives, regulations, and policies. Updating literacy training content on a regular basis ensures that the content remains relevant. Events that may precipitate an update to literacy training content include

assessment or audit findings, security incidents or breaches, or changes in applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

Potential indicators and possible precursors of insider threats include behaviors such as inordinate, long-term job dissatisfaction; attempts to gain access to information that is not required for job performance; unexplained access to financial resources; sexual harassment or bullying of fellow employees; workplace violence; and other serious violations of the policies, procedures, rules, directives, or practices of organizations. Organizations may consider tailoring insider threat awareness topics to roles (e.g., training for managers may be focused on specific changes in the behavior of team members, while training for employees may be focused on more general observations).

Social engineering is an attempt to deceive an individual into revealing information or taking an action that can be used to breach, compromise, or otherwise adversely impact a system. Social engineering includes phishing, pretexting, impersonation, baiting, quid pro quo, threadjacking, social media exploitation, and tailgating. Social mining is an attempt to gather information about the organization that may be used to support future attacks. Security literacy training includes how to communicate employee and management concerns regarding potential indicators of insider threat and potential and actual instances of social engineering and data mining through appropriate organizational channels in accordance with established policies and procedures.

REFERENCES

Source Controls: AT-02, AT-02(02), AT-02(03)

Supporting Publications: SP 800-50 [32], SP 800-160-2 [10]

03.02.02 Role-Based Training

a. Provide role-based security training to organizational personnel:
    1. Before authorizing access to the system or CUI, before performing assigned duties, and [*Assignment: organization-defined frequency*] thereafter
    2. When required by system changes or following [*Assignment: organization-defined events*].
b. Update role-based training content [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

DISCUSSION

Organizations determine the content and frequency of security training based on the assigned duties, roles, and responsibilities of individuals and the security requirements of the systems to which personnel have authorized access. In addition,

organizations provide system developers, enterprise architects, security architects, software developers, systems integrators, acquisition/procurement officials, system and network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation, security assessors, and personnel with access to system-level software with security-related technical training specifically tailored for their assigned duties.

Comprehensive role-based training addresses management, operational, and technical roles and responsibilities that cover physical, personnel, and technical controls. Such training can include policies, procedures, tools, and artifacts for the security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs.

REFERENCES

Source Control: AT-03

Supporting Publications: SP 800-161 [33], SP 800-181 [34]

03.02.03 Withdrawn

Incorporated into 03.02.01.

3.3. Audit and Accountability

03.03.01 Event Logging

a. Specify the following event types selected for logging within the system: [*Assignment: organization-defined event types*].

b. Review and update the event types selected for logging [*Assignment: organization-defined frequency*].

DISCUSSION

An event is any observable occurrence in a system, including unlawful or unauthorized system activity. Organizations identify event types for which a logging functionality is needed. This includes events that are relevant to the security of systems and the environments in which those systems operate to meet specific and ongoing auditing needs. Event types can include password changes, the execution of privileged functions, failed logons or accesses related to systems, administrative privilege usage, or third-party credential usage. In determining event types that require logging, organizations consider the system monitoring and auditing that are appropriate for each of the security requirements. When defining event types, organizations consider the logging necessary to cover related events, such as the

steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented or cloud-based architectures.

Monitoring and auditing requirements can be balanced with other system needs. For example, organizations may determine that systems must have the capability to log every file access — both successful and unsuccessful — but only activate that capability under specific circumstances due to the potential burden on system performance. The event types that are logged by organizations may change over time. Reviewing and updating the set of logged event types are necessary to ensure that the current set of event types remains relevant.

REFERENCES

Source Control: AU-02

Supporting Publications: SP 800-92 [35]

03.03.02 Audit Record Content

a. Include the following content in audit records:
    1. What type of event occurred
    2. When the event occurred
    3. Where the event occurred
    4. Source of the event
    5. Outcome of the event
    6. Identity of the individuals, subjects, objects, or entities associated with the event
b. Provide additional information for audit records as needed.

DISCUSSION

Audit record content that may be necessary to support the auditing function includes time stamps, source and destination addresses, user or process identifiers, event descriptions, file names, and the access control or flow control rules that are invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the system after the event occurred). Detailed information that organizations consider in audit records may include a full text recording of privileged commands or the individual identities of group account users.

REFERENCES

Source Controls: AU-03, AU-03(01)

Supporting Publications: None

03.03.03 Audit Record Generation

a. Generate audit records for the selected event types and audit record content specified in 03.03.01 and 03.03.02.

b. Retain audit records for a time period consistent with the records retention policy.

DISCUSSION

Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit logging capability and can facilitate the identification of root causes to problems. The ability to add information generated in audit records is dependent on system functionality to configure the audit record content. Organizations may consider additional information in audit records, including the access control or flow control rules invoked and the individual identities of group account users. Organizations may also consider limiting additional audit record information to only information that is explicitly needed for audit requirements.

REFERENCES

Source Controls: AU-11, AU-12

Supporting Publications: SP 800-92 [35]

03.03.04 Response to Audit Logging Process Failures

a. Alert organizational personnel or roles within [*Assignment: organization-defined time period*] in the event of an audit logging process failure.

b. Take the following additional actions: [*Assignment: organization-defined additional actions*].

DISCUSSION

Audit logging process failures include software and hardware errors, failures in audit log capturing mechanisms, and reaching or exceeding audit log storage capacity. Response actions include overwriting the oldest audit records, shutting down the system, and stopping the generation of audit records. Organizations may choose to define additional actions for audit logging process failures based on the type of failure, the location of the failure, the severity of the failure, or a combination of

such factors. When the audit logging process failure is related to storage, the response is carried out for the audit log storage repository (i.e., the distinct system component where the audit logs are stored), the system on which the audit logs reside, the total audit log storage capacity of the organization (i.e., all audit log storage repositories combined), or all three. Organizations may decide to take no additional actions after alerting designated roles or personnel.

REFERENCES

Source Control: AU-05

Supporting Publications: None

03.03.05 Audit Record Review, Analysis, and Reporting

a. Review and analyze system audit records [*Assignment: organization-defined frequency*] for indications and the potential impact of inappropriate or unusual activity.

b. Report findings to organizational personnel or roles.

c. Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

DISCUSSION

Audit record review, analysis, and reporting cover information security logging performed by organizations and can include logging that results from the monitoring of account usage, remote access, wireless connectivity, configuration settings, the use of maintenance tools and nonlocal maintenance, system component inventory, mobile device connection, equipment delivery and removal, physical access, temperature and humidity, communications at system interfaces, and the use of mobile code. Findings can be reported to organizational entities, such as the incident response team, help desk, and security or privacy offices. If organizations are prohibited from reviewing and analyzing audit records or unable to conduct such activities, the review or analysis may be carried out by other organizations granted such authority. The scope, frequency, and/or depth of the audit record review, analysis, and reporting may be adjusted to meet organizational needs based on new information received. Correlating audit record review, analysis, and reporting processes helps to ensure that audit records collectively create a more complete view of events.

REFERENCES

Source Controls: AU-06, AU-06(03)

Supporting Publications: SP 800-86 [36], SP 800-101 [37]

03.03.06 Audit Record Reduction and Report Generation

a. Implement an audit record reduction and report generation capability that supports audit record review, analysis, reporting requirements, and after-the-fact investigations of incidents.

b. Preserve the original content and time ordering of audit records.

DISCUSSION

Audit records are generated in 03.03.03. Audit record reduction and report generation occur after audit record generation. Audit record reduction is a process that manipulates collected audit information and organizes it in a summary format that is more meaningful to analysts. Audit record reduction and report generation capabilities do not always come from the same system or organizational entities that conduct auditing activities. An audit record reduction capability can include, for example, modern data mining techniques with advanced data filters to identify anomalous behavior in audit records. The report generation capability provided by the system can help generate customizable reports. The time ordering of audit records can be a significant issue if the granularity of the time stamp in the record is insufficient.

REFERENCES

Source Control: AU-07

Supporting Publications: None

03.03.07 Time Stamps

a. Use internal system clocks to generate time stamps for audit records.

b. Record time stamps for audit records that meet [*Assignment: organization-defined granularity of time measurement*] and that use Coordinated Universal Time (UTC), have a fixed local time offset from UTC, or include the local time offset as part of the time stamp.

DISCUSSION

Time stamps generated by the system include the date and time. Time is often expressed in Coordinated Universal Time (UTC) — a modern continuation of Greenwich Mean Time (GMT) — or local time with an offset from UTC. The granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks (e.g., clocks synchronizing within hundreds or tens of milliseconds). Organizations may define different time granularities for system components. Time service can be critical to other security capabilities (e.g., access control and identification and authentication), depending on the nature of the mechanisms used to support those capabilities.