CHAPTER ONE

INTRODUCTION

THE NEED TO PROTECT CONTROLLED UNCLASSIFIED INFORMATION

Today, more than at any time in history, the federal government is relying on external service providers to help carry out a wide range of federal missions and business functions using information systems.[1] Many federal contractors process, store, and transmit sensitive federal information to support the delivery of essential products and services to federal agencies (e.g., providing financial services; providing web and electronic mail services; processing security clearances or healthcare data; providing cloud services; and developing communications, satellite, and weapons systems). Federal information is frequently provided to or shared with entities such as state and local governments, colleges and universities, and independent research organizations. The protection of sensitive federal information while residing in *nonfederal systems*[2] and organizations is of paramount importance to federal agencies, and can directly impact the ability of the federal government to carry out its designated missions and business operations.

The protection of unclassified federal information in nonfederal systems and organizations is dependent on the federal government providing a process for identifying the different types of information that are used by federal agencies. [EO 13556] established a governmentwide Controlled Unclassified Information (CUI)[3] Program to standardize the way the executive branch handles unclassified information that requires protection.[4] Only information that requires safeguarding or dissemination controls pursuant to federal law, regulation, or governmentwide policy may be designated as CUI. The CUI Program is designed to address several deficiencies in managing and protecting unclassified information to include inconsistent markings, inadequate safeguarding, and needless restrictions, both by standardizing procedures and by providing common definitions through a CUI Registry [NARA CUI]. The CUI Registry is the online repository for information, guidance, policy, and requirements on handling CUI, including issuances by the CUI Executive Agent. The CUI Registry identifies approved CUI categories, provides general descriptions for each, identifies the basis for controls, and sets out procedures for the use of CUI including, but not limited to, marking, safeguarding, transporting, disseminating, reusing, and disposing of the information.

[1] An *information system* is a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems also include specialized systems, for example: industrial/process control systems, cyber-physical systems, embedded systems, and devices. The term *system* is used throughout this publication to represent all types of computing platforms that can process, store, or transmit CUI.

[2] 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. A system that does not meet such criteria is a *nonfederal system*.

[3] *Controlled Unclassified Information* is any information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under [EO 13526] or any predecessor or successor order, or [ATOM54], as amended.

[4] [EO 13556] designated the National Archives and Records Administration (NARA) as the Executive Agent to implement the CUI Program.

[EO 13556] also required that the CUI Program emphasize openness, transparency, and uniformity of governmentwide practices, and that the implementation of the program take place in a manner consistent with applicable policies established by the Office of Management and Budget (OMB) and federal standards and guidelines issued by the National Institute of Standards and Technology (NIST). The federal CUI *regulation*,[5] developed by the CUI Executive Agent, provides guidance to federal agencies on the designation, safeguarding, dissemination, marking, decontrolling, and disposition of CUI, establishes self-inspection and oversight requirements, and delineates other facets of the program.

1.1 PURPOSE AND APPLICABILITY

The purpose of this publication is to provide federal agencies with recommended security requirements[6] for protecting the *confidentiality* of CUI: (1) when the CUI is resident in a nonfederal system and organization; (2) when the nonfederal organization is *not* collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency;[7] and (3) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry.[8]

The requirements apply to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components.[9] If nonfederal organizations designate specific system components for the processing, storage, or transmission of CUI, those organizations may limit the scope of the security requirements by isolating the designated system components in a separate CUI *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 the CUI and avoid increasing the organization's security posture to a level beyond that which it requires for protecting its missions, operations, and assets.

[5] [32 CFR 2002] was issued on September 14, 2016 and became effective on November 14, 2016.

[6] The term *requirements* can be used in different contexts. In the context of federal information security and privacy policies, the term is generally used to refer to information security and privacy obligations imposed on organizations. For example, OMB Circular A-130 imposes a series of information security and privacy requirements with which federal agencies must comply when managing information resources. In addition to the use of the term requirements in the context of federal policy, the term requirements is used in this guideline in a broader sense to refer to an expression of the set of stakeholder protection needs for a particular system or organization. Stakeholder protection needs and corresponding security requirements may be derived from many sources (e.g., laws, executive orders, directives, regulations, policies, standards, mission and business needs, or risk assessments). The term requirements, as used in this guideline, includes both legal and policy requirements, as well as an expression of the broader set of stakeholder protection needs that may be derived from other sources. All of these requirements, when applied to a system, help determine the required characteristics of the system.

[7] 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], including the requirements in [FIPS 200] and the security controls in [SP 800-53] (See [44 USC 3554] (a)(1)(A)).

[8] The requirements in this publication can be used to comply with the [FISMA] requirement for senior agency officials to provide information security for the information that supports the operations and assets under their control, including CUI that is resident in nonfederal systems and organizations (See [44 USC 3554] (a)(1)(A) and (a)(2)).

[9] System *components* include, for example: mainframes, workstations, servers; input and output devices; network components; operating systems; virtual machines; and applications.

The recommended security requirements in this publication are intended for use by federal agencies in appropriate contractual vehicles or other agreements established between those agencies and nonfederal organizations. In CUI guidance and the CUI Federal Acquisition Regulation (FAR),[10] the CUI Executive Agent will address determining compliance with security requirements.[11]

In accordance with the federal CUI regulation, federal agencies using federal systems to process, store, or transmit CUI, at a minimum, must comply with:

- Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (moderate confidentiality);[12]
- Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*;
- NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*; and
- NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*.

The responsibility of federal agencies to protect CUI does not change when such information is shared with nonfederal partners. Therefore, a similar level of protection is needed when CUI is processed, stored, or transmitted by *nonfederal organizations* using nonfederal systems.[13] The recommended requirements for safeguarding CUI in nonfederal systems and organizations are derived from the above authoritative federal standards and guidelines to maintain a consistent level of protection. However, recognizing that the scope of the safeguarding requirements in the federal CUI regulation is limited to the security objective of confidentiality (i.e., not directly addressing integrity and availability) and that some of the security requirements expressed in the NIST standards and guidelines are uniquely federal, the requirements in this publication have been *tailored* for nonfederal entities.

The tailoring criteria described in Chapter Two are not intended to reduce or minimize the federal requirements for the safeguarding of CUI as expressed in the federal CUI regulation. Rather, the intent is to express the requirements in a manner that allows for and facilitates the equivalent safeguarding measures within nonfederal systems and organizations and does not diminish the level of protection of CUI required for moderate confidentiality. Additional or differing requirements, other than the requirements described in this publication, may be applied only when such requirements are based on law, regulation, or governmentwide policy and when indicated in the CUI Registry as CUI-specified or when an agreement establishes

[10] NARA, as the CUI Executive Agent, plans to sponsor a single FAR clause that will apply the requirements of the federal CUI regulation and NIST Special Publication 800-171 to contractors. Until the FAR clause is in place, the requirements in NIST Special Publication 800-171 may be referenced in federal contracts consistent with federal law and regulatory requirements.

[11] [SP 800-171A] provides assessment procedures to determine compliance to the CUI security requirements.

[12] [FIPS 199] defines three values of potential impact (i.e., low, moderate, high) on organizations, assets, or individuals in the event of a breach of security (e.g., a loss of confidentiality).

[13] A *nonfederal organization* is any entity that owns, operates, or maintains a nonfederal system. Examples include: state, local, and tribal governments; colleges and universities; and contractors.

requirements to protect CUI Basic[14] at higher than moderate confidentiality. The provision of safeguarding requirements for CUI in a specified category will be addressed by the National Archives and Records Administration (NARA) in its CUI guidance and in the CUI FAR; and reflected as specific requirements in contracts or other agreements. Nonfederal organizations may use the same CUI infrastructure for multiple government contracts or agreements, if the CUI infrastructure meets the safeguarding requirements for the organization's CUI-related contracts and/or agreements including any specific safeguarding required or permitted by the authorizing law, regulation, or governmentwide policy.

1.2 TARGET AUDIENCE

This publication serves a diverse group of individuals and organizations in both the public and private sectors including, but not limited to, 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);
- Acquisition or procurement responsibilities (e.g., contracting officers);
- System, security, or risk management and oversight responsibilities (e.g., authorizing officials, chief information officers, chief information security officers, system owners, information security managers); and
- Security assessment and monitoring responsibilities (e.g., auditors, system evaluators, assessors, independent verifiers/validators, analysts).

The above roles and responsibilities can be viewed from two distinct perspectives: the *federal perspective* as the entity establishing and conveying the security requirements in contractual vehicles or other types of inter-organizational agreements; and the *nonfederal perspective* as the entity responding to and complying with the security requirements set forth in contracts or agreements.

1.3 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes the fundamental assumptions and methodology used to develop the security requirements for protecting the confidentiality of CUI; the format and structure of the requirements; and the tailoring criteria applied to the NIST standards and guidelines to obtain the requirements.
- **Chapter Three** describes the fourteen families of security requirements for protecting the confidentiality of CUI in nonfederal systems and organizations.
- **Supporting appendices** provide additional information related to the protection of CUI in nonfederal systems and organizations including: general references; definitions and terms; acronyms; mapping tables relating security requirements to the security controls in [SP 800-53] and [ISO 27001]; and tailoring actions applied to the moderate security control baseline.

[14] CUI Basic is defined in the CUI Registry [NARA CUI].

CHAPTER TWO

THE FUNDAMENTALS

ASSUMPTIONS AND METHODOLOGY FOR DEVELOPING SECURITY REQUIREMENTS

This chapter describes the assumptions and the methodology used to develop the recommended security requirements to protect CUI in nonfederal systems and organizations; the structure of the basic and derived security requirements; and the tailoring criteria applied to the federal information security requirements and controls.

2.1 BASIC ASSUMPTIONS

The recommended security requirements described in this publication have been developed based on three fundamental assumptions:

- Statutory and regulatory requirements for the protection of CUI are *consistent*, whether such information resides in federal systems or nonfederal systems including the environments in which those systems operate;
- Safeguards implemented to protect CUI are *consistent* in both federal and nonfederal systems and organizations; and
- The confidentiality impact value for CUI is no less than [FIPS 199] *moderate*.[15] [16]

The assumptions reinforce the concept that federal information designated as CUI has the same intrinsic *value* and potential *adverse impact* if compromised—whether such information resides in a federal or a nonfederal organization. Thus, protecting the confidentiality of CUI is critical to the mission and business success of federal agencies and the economic and national security interests of the nation. Additional assumptions also impacting the development of the security requirements and the expectation of federal agencies in working with nonfederal entities include:

- Nonfederal organizations have information technology infrastructures in place, and are not necessarily developing or acquiring systems specifically for processing, storing, or transmitting CUI;
- Nonfederal organizations have specific safeguarding measures in place to protect their information which may also be sufficient to satisfy the security requirements;
- Nonfederal organizations may not have the necessary organizational structure or resources to satisfy every security requirement and may implement alternative, but equally effective, security measures to compensate for the inability to satisfy a requirement; and
- Nonfederal organizations can implement a variety of potential security solutions directly or using external service providers (e.g., managed services) to satisfy security requirements.

[15] The moderate impact *value* defined in [FIPS 199] may become part of a moderate impact *system* in [FIPS 200], which requires the use of the moderate baseline in [SP 800-53] as the starting point for tailoring actions.

[16] In accordance with [32 CFR 2002], CUI is categorized at no less than the moderate confidentiality impact value. However, when federal law, regulation, or governmentwide policy establishing the control of the CUI specifies controls that differ from those of the moderate confidentiality baseline, then these will be followed.

IMPLEMENTING A SINGLE STATE SECURITY SOLUTION FOR CUI

Controlled Unclassified Information has the *same value*, whether such information is resident in a federal system that is part of a federal agency or a nonfederal system that is part of a nonfederal organization. Accordingly, the recommended security requirements contained in this publication are consistent with and are complementary to the standards and guidelines used by federal agencies to protect CUI.

2.2 DEVELOPMENT OF SECURITY REQUIREMENTS

The security requirements for protecting the confidentiality of CUI in nonfederal systems and organizations have a well-defined structure that consists of a *basic security requirements* section and a *derived security requirements* section. The basic security requirements are obtained from [FIPS 200], which provides the high-level and fundamental security requirements for federal information and systems. The derived security requirements, which supplement the basic security requirements, are taken from the security controls in [SP 800-53]. Starting with the security requirements and the security controls in the moderate baseline (i.e., the minimum level of protection required for CUI in federal systems and organizations), the requirements and controls are *tailored* to eliminate requirements, controls, or parts of controls that are:

- Uniquely federal (i.e., primarily the responsibility of the federal government);
- Not directly related to protecting the confidentiality of CUI; or
- Expected to be routinely satisfied by nonfederal organizations without specification.[17]

Appendix E provides a complete listing of security controls that support the CUI derived security requirements and those controls that have been eliminated from the moderate baseline based on the CUI tailoring criteria described above.

The combination of the basic and derived security requirements captures the intent of [FIPS 200] and [SP 800-53] with respect to the protection of the *confidentiality* of CUI in nonfederal systems and organizations. Appendix D provides informal mappings of the security requirements to the relevant security controls in [SP 800-53] and [ISO 27001]. The mappings promote a better understanding of the CUI security requirements, and are *not* intended to impose additional requirements on nonfederal organizations.

[17] The security requirements developed from the tailored [FIPS 200] security requirements and the [SP 800-53] moderate security control baseline represent a subset of the safeguarding measures that are necessary for a *comprehensive* information security program. The strength and quality of such programs in nonfederal organizations depend on the degree to which the organizations implement the security requirements and controls that are expected to be routinely satisfied without specification by the federal government. This includes implementing security policies, procedures, and practices that support an effective risk-based information security program. Nonfederal organizations are encouraged to refer to Appendix E and [SP 800-53] for a complete listing of security controls in the moderate baseline deemed out of scope for the security requirements in Chapter Three.

The following *Media Protection* family example illustrates the structure of a CUI requirement:

Basic Security Requirements

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

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

3.8.3 Sanitize or destroy 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.

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 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.

For ease of use, the security requirements are organized into fourteen *families*. Each family contains the requirements related to the general security topic of the family. The families are closely aligned with the minimum-security requirements for federal information and systems described in [FIPS 200]. The *contingency planning*, *system and services acquisition*, and *planning* requirements are not included within the scope of this publication due to the tailoring criteria.[18] Table 1 lists the security requirement families addressed in this publication.

TABLE 1: SECURITY REQUIREMENT FAMILIES

FAMILY	FAMILY
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

[18] Three exceptions include: a requirement to protect the confidentiality of system backups (derived from CP-9) from the *contingency planning* family; a requirement to develop and implement a system security plan (derived from PL-2) from the *planning* family; and a requirement to implement system security engineering principles (derived from SA-8) from the *system and services acquisition* family. The requirements are included in the CUI *media protection*, *security assessment*, and *system and communications protection* requirements families, respectively.

A *discussion* section follows each CUI security requirement providing additional information to facilitate the implementation and assessment of the requirements. This information is derived primarily from the security controls discussion sections in [SP 800-53] and is provided to give organizations a better understanding of the mechanisms and procedures used to implement the controls used to protect CUI. The discussion section is *informative*, not *normative*. It is not intended to extend the scope of a requirement or to influence the solutions organizations may use to satisfy a requirement. The use of examples is notional, not exhaustive, and not reflective of potential options available to organizations. Figure 1 illustrates basic security requirement 3.8.3 with its supporting discussion section and informative references.

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

DISCUSSION

This requirement applies to all system media, digital and non-digital, subject to disposal or reuse. Examples include: digital media found in workstations, network components, scanners, copiers, printers, notebook computers, and mobile devices; and non-digital media such as paper and microfilm. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is released for reuse or disposal.

Organizations determine the appropriate sanitization methods, recognizing that destruction may be necessary when other methods cannot be applied to the media requiring sanitization. Organizations use discretion on the employment of sanitization techniques and procedures for media containing information that is in the public domain or publicly releasable or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing CUI from documents, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing the words or sections from the document. NARA policy and guidance control sanitization processes for controlled unclassified information.

[SP 800-88] provides guidance on media sanitization.

FIGURE 1: FORMAT AND STRUCTURE OF CUI SECURITY REQUIREMENT

CHAPTER THREE

THE REQUIREMENTS

SECURITY REQUIREMENTS FOR PROTECTING THE CONFIDENTIALITY OF CUI

This chapter describes fourteen families of recommended security requirements for protecting the confidentiality of CUI in nonfederal systems and organizations.[19] The security controls from [SP 800-53] associated with the basic and derived requirements are listed in Appendix D.[20] Organizations can use the NIST publication to obtain additional, non-prescriptive information related to the recommended security requirements (e.g., explanatory information in the discussion section for each of the referenced security controls, mapping tables to [ISO 27001] security controls, and a catalog of optional controls that can be used to specify additional security requirements, if needed). This information can help clarify or interpret the requirements in the context of mission and business requirements, operational environments, or assessments of risk. Nonfederal organizations can implement a variety of potential security solutions either directly or using managed services, to satisfy the security requirements and may implement alternative, but equally effective, security measures to compensate for the inability to satisfy a requirement.[21]

DISCUSSION SECTION

The discussion section associated with each CUI requirement is *informative*, not *normative*. It is not intended to extend the scope of a requirement or to influence the solutions organizations may use to satisfy a requirement. In addition, the use of examples is notional, not exhaustive, and not reflective of potential options available to organizations.

Nonfederal organizations describe, in a system security plan, how the security requirements are met or how organizations plan to meet the requirements and address known and anticipated threats. The system security plan describes: the system boundary; operational environment; how security requirements are implemented; and the relationships with or connections to other systems. Nonfederal organizations develop plans of action that describe how unimplemented security requirements will be met and how any planned mitigations will be implemented. Organizations can document the system security plan and the plan of action as separate or combined documents and in any chosen format.[22]

[19] The security objectives of confidentiality and integrity are closely related since many of the underlying security mechanisms at the system level support both objectives. Therefore, the basic and derived security requirements in this publication provide protection from unauthorized disclosure and unauthorized modification of CUI.

[20] The security control references in Appendix D are included to promote a better understanding of the recommended security requirements and do not expand the scope of the requirements.

[21] To promote consistency, transparency, and comparability, the compensatory security measures selected by organizations are based on or derived from *existing* and *recognized* security standards and control sets, including, for example, [ISO 27001] or [SP 800-53].

[22] [NIST CUI] provides supplemental material for Special Publication 800-171 including templates for system security plans and plans of action.

When requested, the system security plan (or extracts thereof) and the associated plans of action for any planned implementations or mitigations are submitted to the responsible federal agency/contracting office to demonstrate the nonfederal organization's implementation or planned implementation of the security requirements. Federal agencies may consider the submitted system security plans and plans of action as critical inputs to a risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the nonfederal organization.

The recommended security requirements in this publication apply only to the components of nonfederal systems that process, store, or transmit CUI or that provide protection for such components. 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 3.12.4, is used to describe any enduring exceptions to the security requirements. Individual, isolated, or temporary deficiencies are managed though plans of action, as reflected in requirement 3.12.2.

THE MEANING OF ORGANIZATIONAL SYSTEMS

The term *organizational system* is used in many of the recommended CUI security requirements in this publication. This term has a specific meaning regarding the scope of applicability for the security requirements. The requirements apply only to the components of nonfederal systems that process, store, or transmit CUI, or that provide protection for the system components. The appropriate scoping for the CUI security requirements is an important factor in determining protection-related investment decisions and managing security risk for nonfederal organizations that have the responsibility of safeguarding CUI.

3.1 ACCESS CONTROL

Basic Security Requirements

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

DISCUSSION

Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. This requirement focuses on account management for systems and applications. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged verses non-privileged) are addressed in requirement 3.1.2.

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

DISCUSSION

Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. System account types include individual, shared, group, system, anonymous, guest, emergency, developer, manufacturer, vendor, and temporary. Other attributes required for authorizing access include restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., system upgrades scheduled maintenance,) and mission or business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements).

Derived Security Requirements

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

DISCUSSION

Information flow control regulates where information can travel within a system and between systems (versus who can access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include the following: keeping export-controlled information from being transmitted in the clear to the Internet; blocking outside traffic that claims to be from within the organization; restricting requests to the Internet that are not from the internal web proxy server; and limiting information transfers between organizations based on data structures and content.

Organizations commonly use information flow control policies and enforcement mechanisms to control the flow of information 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., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict system services, provide a packet-filtering capability based on header information, or 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.

Transferring information between systems representing different security domains with different security policies introduces 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 information transfers between interconnected systems (i.e., allowing access only); employing hardware mechanisms to enforce one-way information flows; and implementing trustworthy regrading mechanisms to reassign security attributes and security labels.

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

DISCUSSION

Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes dividing mission functions and system support functions among different individuals or roles; conducting system support functions with different individuals (e.g., configuration management, quality assurance and testing, system management, programming, and network security); and ensuring that security personnel administering 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 organizational systems and system components when developing policy on separation of duties.

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

DISCUSSION

Organizations employ the principle of least privilege for specific duties and authorized accesses for users and processes. The principle of least privilege is applied with the goal of authorized privileges no higher than necessary to accomplish required organizational missions or business functions. Organizations consider the creation of additional processes, roles, and system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational systems. Security functions include establishing system accounts, setting events to be logged, setting intrusion detection parameters, and configuring access authorizations (i.e., permissions, privileges).

Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information or functions. Organizations may differentiate in the application of this requirement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk.

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

DISCUSSION

This requirement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account.

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

DISCUSSION

Privileged functions include establishing system accounts, performing system integrity checks, conducting patching operations, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users. Note that this requirement represents a condition to be achieved by the definition of authorized privileges in 3.1.2.

Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Logging the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat.

3.1.8 Limit unsuccessful logon attempts.

DISCUSSION

This requirement applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by systems are, in most cases, temporary and automatically release after a predetermined period established by the

organization (i.e., a delay algorithm). If a delay algorithm is selected, organizations may employ different algorithms for different system components based on the capabilities of the respective components. Responses to unsuccessful logon attempts may be implemented at the operating system and application levels.

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

DISCUSSION

System use notifications can be implemented using messages or warning banners displayed before individuals log in to organizational systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Based on a risk assessment, organizations consider whether a secondary system use notification is needed to access applications or other system resources after the initial network logon. Where necessary, posters or other printed materials may be used in lieu of an automated system banner. Organizations consult with the Office of General Counsel for legal review and approval of warning banner content.

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

DISCUSSION

Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of the system but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined, typically at the operating system level (but can also be at the application level). Session locks are not an acceptable substitute for logging out of the system, for example, if organizations require users to log out at the end of the workday.

Pattern-hiding displays can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey controlled unclassified information.

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

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). A logical session (for local, network, and remote access) is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated (and thus terminate user access) without terminating network sessions. Session termination terminates all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated. Conditions or trigger events requiring automatic session termination can include organization-defined periods of user inactivity, targeted responses to certain types of incidents, and time-of-day restrictions on system use.

3.1.12 Monitor and control remote access sessions.

DISCUSSION

Remote access is access to organizational systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with

appropriate control (e.g., employing encryption techniques for confidentiality protection), may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. VPNs with encrypted tunnels can affect the capability to adequately monitor network communications traffic for malicious code.

Automated monitoring and control of remote access sessions allows organizations to detect cyber-attacks and help to ensure ongoing compliance with remote access policies by auditing connection activities of remote users on a variety of system components (e.g., servers, workstations, notebook computers, smart phones, and tablets).

[SP 800-46], [SP 800-77], and [SP 800-113] provide guidance on secure remote access and virtual private networks.

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

DISCUSSION

Cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. See [NIST CRYPTO]; [NIST CAVP]; [NIST CMVP]; National Security Agency Cryptographic Standards.

3.1.14 Route remote access via managed access control points.

DISCUSSION

Routing remote access through managed access control points enhances explicit, organizational control over such connections, reducing the susceptibility to unauthorized access to organizational systems resulting in the unauthorized disclosure of CUI.

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

DISCUSSION

A privileged command is a human-initiated (interactively or via a process operating on behalf of the human) command executed on a system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information. Security-relevant information is any information within the system 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. Controlling such access from remote locations helps to ensure that unauthorized individuals are not able to execute such commands freely with the potential to do serious or catastrophic damage to organizational systems. Note that the ability to affect the integrity of the system is considered security-relevant as that could enable the means to by-pass security functions although not directly impacting the function itself.

3.1.16 Authorize wireless access prior to allowing such connections.

DISCUSSION

Establishing usage restrictions and configuration/connection requirements for wireless access to the system provides criteria for organizations to support wireless access authorization decisions. Such restrictions and requirements reduce the susceptibility to unauthorized access to the system through wireless technologies. Wireless networks use authentication protocols which provide credential protection and mutual authentication.

[SP 800-97] provide guidance on secure wireless networks.

3.1.17 Protect wireless access using authentication and encryption.

DISCUSSION

Organizations authenticate individuals and devices to help protect wireless access to the system. Special attention is given to the wide variety of devices that are part of the Internet of Things with potential wireless access to organizational systems. See [NIST CRYPTO].

3.1.18 Control connection of mobile devices.

DISCUSSION

A mobile device is a computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local, non-removable or removable data storage; and includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture information, or built-in features for synchronizing local data with remote locations. Examples of mobile devices include smart phones, e-readers, and tablets.

Due to the large variety of mobile devices with different technical characteristics and capabilities, organizational restrictions may vary for the different types of devices. Usage restrictions and implementation guidance for mobile devices include: device identification and authentication; configuration management; implementation of mandatory protective software (e.g., malicious code detection, firewall); scanning devices for malicious code; updating virus protection software; scanning for critical software updates and patches; conducting primary operating system (and possibly other resident software) integrity checks; and disabling unnecessary hardware (e.g., wireless, infrared). The need to provide adequate security for mobile devices goes beyond this requirement. Many controls for mobile devices are reflected in other CUI security requirements.

[SP 800-124] provides guidance on mobile device security.

3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.[23]

DISCUSSION

Organizations can employ full-device encryption or container-based encryption to protect the confidentiality of CUI on mobile devices and computing platforms. Container-based encryption provides a more fine-grained approach to the encryption of data and information including encrypting selected data structures such as files, records, or fields. See [NIST CRYPTO].

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

DISCUSSION

External systems are systems or components of systems for which organizations typically have no direct supervision and authority over the application of security requirements and controls or the determination of the effectiveness of implemented controls on those systems. External systems include personally owned systems, components, or devices and privately-owned computing and communications devices resident in commercial or public facilities. This requirement also addresses the use of external systems for the processing, storage, or transmission of CUI, including accessing cloud services (e.g., infrastructure as a service, platform as a service, or software as a service) from organizational systems.

Organizations establish terms and conditions for the use of external systems in accordance with organizational security policies and procedures. Terms and conditions address as a minimum, the types of applications that can be accessed on organizational systems from external systems. If

[23] Mobile devices and computing platforms include, for example, smartphones and tablets.

terms and conditions with the owners of external systems cannot be established, organizations may impose restrictions on organizational personnel using those external systems.

This requirement recognizes that there are circumstances where individuals using external systems (e.g., contractors, coalition partners) need to access organizational systems. In those situations, organizations need confidence that the external systems contain the necessary controls so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required controls have been effectively implemented can be achieved by third-party, independent assessments, attestations, or other means, depending on the assurance or confidence level required by organizations.

Note that while "external" typically refers to outside of the organization's direct supervision and authority, that is not always the case. Regarding the protection of CUI across an organization, the organization may have systems that process CUI and others that do not. And among the systems that process CUI there are likely access restrictions for CUI that apply between systems. Therefore, from the perspective of a given system, other systems within the organization may be considered "external" to that system.

3.1.21 **Limit use of portable storage devices on external systems.**

DISCUSSION

Limits on the use of organization-controlled portable storage devices in external systems include complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used. Note that while "external" typically refers to outside of the organization's direct supervision and authority, that is not always the case. Regarding the protection of CUI across an organization, the organization may have systems that process CUI and others that do not. Among the systems that process CUI there are likely access restrictions for CUI that apply between systems. Therefore, from the perspective of a given system, other systems within the organization may be considered "external" to that system.

3.1.22 **Control CUI posted or processed on publicly accessible systems.**

DISCUSSION

In accordance with laws, Executive Orders, directives, policies, regulations, or standards, the public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act, CUI, and proprietary information). This requirement addresses systems that are controlled by the organization and accessible to the public, typically without identification or authentication. Individuals authorized to post CUI onto publicly accessible systems are designated. The content of information is reviewed prior to posting onto publicly accessible systems to ensure that nonpublic information is not included.

3.2 AWARENESS AND TRAINING

Basic Security Requirements

3.2.1 **Ensure that managers, systems administrators, and users of organizational 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 systems.**

DISCUSSION

Organizations determine the content and frequency of security awareness training and security awareness techniques based on the specific organizational requirements and the systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security

incidents. The content also addresses awareness of the need for operations security. Security awareness techniques include: formal training; offering supplies inscribed with security reminders; generating email advisories or notices from organizational officials; displaying logon screen messages; displaying security awareness posters; and conducting information security awareness events.

[SP 800-50] provides guidance on security awareness and training programs.

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

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

Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering 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.

[SP 800-181] provides guidance on role-based information security training in the workplace. [SP 800-161] provides guidance on supply chain risk management.

Derived Security Requirements

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

DISCUSSION

Potential indicators and possible precursors of insider threat 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; bullying or sexual harassment of fellow employees; workplace violence; and other serious violations of the policies, procedures, directives, rules, or practices of organizations. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures. Organizations may consider tailoring insider threat awareness topics to the role (e.g., training for managers may be focused on specific changes in behavior of team members, while training for employees may be focused on more general observations).

3.3 AUDIT AND ACCOUNTABILITY

Basic Security Requirements

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

DISCUSSION

An event is any observable occurrence in a system, which includes unlawful or unauthorized system activity. Organizations identify event types for which a logging functionality is needed as those events which are significant and 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, failed logons or failed accesses related to systems, administrative privilege usage, or third-party credential usage. In determining event types that require logging, organizations consider the monitoring and auditing appropriate for each of the CUI security requirements. 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 not activate that capability except for specific circumstances due to the potential burden on system performance.

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. Organizations consider in the definition of event types, 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.

Audit record content that may be necessary to satisfy this requirement includes time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, filenames involved, and access control or flow control rules 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 may consider in audit records includes full text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit log information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest. Audit logs are reviewed and analyzed as often as needed to provide important information to organizations to facilitate risk-based decision making.

[SP 800-92] provides guidance on security log management.

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

DISCUSSION

This requirement ensures that the contents of the audit record include the information needed to link the audit event to the actions of an individual to the extent feasible. Organizations consider logging for traceability including results from monitoring of account usage, remote access, wireless connectivity, mobile device connection, communications at system boundaries, configuration settings, physical access, nonlocal maintenance, use of maintenance tools, temperature and humidity, equipment delivery and removal, system component inventory, use of mobile code, and use of Voice over Internet Protocol (VoIP).

Derived Security Requirements

3.3.3 Review and update logged events.

DISCUSSION

The intent of this requirement is to periodically re-evaluate which logged events will continue to be included in the list of events to be logged. The event types that are logged by organizations may change over time. Reviewing and updating the set of logged event types periodically is necessary to ensure that the current set remains necessary and sufficient.

3.3.4 Alert in the event of an audit logging process failure.

DISCUSSION

Audit logging process failures include software and hardware errors, failures in the audit record capturing mechanisms, and audit record storage capacity being reached or exceeded. This requirement applies to each audit record data storage repository (i.e., distinct system component where audit records are stored), the total audit record storage capacity of organizations (i.e., all audit record data storage repositories combined), or both.

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

DISCUSSION

Correlating audit record review, analysis, and reporting processes helps to ensure that they do not operate independently, but rather collectively. Regarding the assessment of a given organizational system, the requirement is agnostic as to whether this correlation is applied at the system level or at the organization level across all systems.

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

DISCUSSION

Audit record reduction is a process that manipulates collected audit information and organizes such information in a summary format that is more meaningful to analysts. Audit record reduction and report generation capabilities do not always emanate from the same system or organizational entities conducting auditing activities. 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. Time ordering of audit records can be a significant issue if the granularity of the time stamp in the record is insufficient.

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

DISCUSSION

Internal system clocks are used to generate time stamps, which include date and time. Time is 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, for example, clocks synchronizing within hundreds of milliseconds or within tens of milliseconds. Organizations may define different time granularities for different system components. Time service can also be critical to other security capabilities such as access control and identification and authentication, depending on the nature of the mechanisms used to support those capabilities. This requirement provides uniformity of time stamps for systems with multiple system clocks and systems connected over a network. See [IETF 5905].

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

DISCUSSION

Audit information includes all information (e.g., audit records, audit log settings, and audit reports) needed to successfully audit system activity. Audit logging tools are those programs and devices used to conduct audit and logging activities. This requirement focuses on the technical protection of audit information and limits the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by media protection and physical and environmental protection requirements.

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

DISCUSSION

Individuals with privileged access to a system and who are also the subject of an audit by that system, may affect the reliability of audit information by inhibiting audit logging activities or modifying audit records. This requirement specifies that privileged access be further defined between audit-related privileges and other privileges, thus limiting the users with audit-related privileges.

3.4 CONFIGURATION MANAGEMENT

Basic Security Requirements

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

DISCUSSION

Baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and changes to systems. Baseline configurations include information about system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and update and patch information on operating systems and applications; and configuration settings and parameters), network topology, and the logical placement of those components within the system architecture. Baseline configurations of systems also reflect the current enterprise architecture. Maintaining effective baseline configurations requires creating new baselines as organizational systems change over time. Baseline configuration maintenance includes reviewing and updating the baseline configuration when changes are made based on security risks and deviations from the established baseline configuration

Organizations can implement centralized system component inventories that include components from multiple organizational systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., system association, system owner). Information deemed necessary for effective accountability of system components includes hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include manufacturer, device type, model, serial number, and physical location.

[SP 800-128] provides guidance on security-focused configuration management.

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

DISCUSSION

Configuration settings are the set of parameters that can be changed in hardware, software, or firmware components of the system that affect the security posture or functionality of the system. Information technology products for which security-related configuration settings can be defined include mainframe computers, servers, workstations, input and output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications.

Security parameters are those parameters impacting the security state of systems including the parameters required to satisfy other security requirements. Security parameters include: registry settings; account, file, directory permission settings; and settings for functions, ports, protocols, and remote connections. Organizations establish organization-wide configuration settings and subsequently derive specific configuration settings for systems. The established settings become part of the systems configuration baseline.

Common secure configurations (also referred to as security configuration checklists, lockdown and hardening guides, security reference guides, security technical implementation guides) provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for specific information technology platforms/products and instructions for configuring those system components to meet operational requirements. Common secure configurations can be developed by a variety of organizations including information technology product developers, manufacturers, vendors, consortia, academia, industry, federal agencies, and other organizations in the public and private sectors.

[SP 800-70] and [SP 800-128] provide guidance on security configuration settings.

Derived Security Requirements

3.4.3 Track, review, approve or disapprove, and log changes to organizational systems.

DISCUSSION

Tracking, reviewing, approving/disapproving, and logging changes is called configuration change control. Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled and unauthorized changes, and changes to remediate vulnerabilities.

Processes for managing configuration changes to systems include Configuration Control Boards or Change Advisory Boards that review and approve proposed changes to systems. For new development systems or systems undergoing major upgrades, organizations consider including representatives from development organizations on the Configuration Control Boards or Change Advisory Boards. Audit logs of changes include activities before and after changes are made to organizational systems and the activities required to implement such changes.

[SP 800-128] provides guidance on configuration change control.

3.4.4 Analyze the security impact of changes prior to implementation.

DISCUSSION

Organizational personnel with information security responsibilities (e.g., system administrators, system security officers, system security managers, and systems security engineers) conduct security impact analyses. Individuals conducting security impact analyses possess the necessary skills and technical expertise to analyze the changes to systems and the associated security ramifications. Security impact analysis may include reviewing security plans to understand security requirements and reviewing system design documentation to understand the implementation of controls and how specific changes might affect the controls. Security impact analyses may also include risk assessments to better understand the impact of the changes and to determine if additional controls are required.

[SP 800-128] provides guidance on configuration change control and security impact analysis.

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

DISCUSSION

Any changes to the hardware, software, or firmware components of systems can potentially have significant effects on the overall security of the systems. Therefore, organizations permit only qualified and authorized individuals to access systems for purposes of initiating changes, including upgrades and modifications. Access restrictions for change also include software libraries.

Access restrictions include physical and logical access control requirements, workflow automation, media libraries, abstract layers (e.g., changes implemented into external interfaces rather than directly into systems), and change windows (e.g., changes occur only during certain specified times). In addition to security concerns, commonly-accepted due diligence for configuration management includes access restrictions as an essential part in ensuring the ability to effectively manage the configuration.

[SP 800-128] provides guidance on configuration change control.

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

DISCUSSION

Systems can provide a wide variety of functions and services. Some of the functions and services routinely provided by default, may not be necessary to support essential organizational missions, functions, or operations. It is sometimes convenient to provide multiple services from single system components. However, doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per component.

Organizations review functions and services provided by systems or components of systems, to determine which functions and services are candidates for elimination. Organizations disable unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of devices, transfer of information, and tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services.

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

DISCUSSION

Restricting the use of nonessential software (programs) includes restricting the roles allowed to approve program execution; prohibiting auto-execute; program blacklisting and whitelisting; or restricting the number of program instances executed at the same time. The organization makes a security-based determination which functions, ports, protocols, and/or services are restricted. Bluetooth, File Transfer Protocol (FTP), and peer-to-peer networking are examples of protocols organizations consider preventing the use of, restricting, or disabling.

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

DISCUSSION

The process used to identify software programs that are not authorized to execute on systems is commonly referred to as blacklisting. The process used to identify software programs that are authorized to execute on systems is commonly referred to as whitelisting. Whitelisting is the stronger of the two policies for restricting software program execution. In addition to whitelisting, organizations consider verifying the integrity of whitelisted software programs using, for example, cryptographic checksums, digital signatures, or hash functions. Verification of whitelisted software can occur either prior to execution or at system startup.

[SP 800-167] provides guidance on application whitelisting.

3.4.9 Control and monitor user-installed software.

DISCUSSION

Users can install software in organizational systems if provided the necessary privileges. To maintain control over the software installed, organizations identify permitted and prohibited actions regarding software installation through policies. Permitted software installations include updates and security patches to existing software and applications from organization-approved "app stores." Prohibited software installations may include software with unknown or suspect pedigrees or software that organizations consider potentially malicious. The policies organizations select governing user-installed software may be organization-developed or provided by some external entity. Policy enforcement methods include procedural methods, automated methods, or both.

3.5 IDENTIFICATION AND AUTHENTICATION

Basic Security Requirements

3.5.1 Identify system users, processes acting on behalf of users, and devices.

DISCUSSION

Common device identifiers include Media Access Control (MAC), Internet Protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared system accounts. Typically, individual identifiers are the user names associated with the system accounts assigned to those individuals. Organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity. In addition, this requirement addresses individual identifiers that are not necessarily associated with system accounts. Organizational devices requiring identification may be defined by type, by device, or by a combination of type/device.

[SP 800-63-3] provides guidance on digital identities.

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

DISCUSSION

Individual authenticators include the following: passwords, key cards, cryptographic devices, and one-time password devices. Initial authenticator content is the actual content of the authenticator, for example, the initial password. In contrast, the requirements about authenticator content include the minimum password length. Developers ship system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk.

Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics including minimum password length, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include certificates and passwords.

[SP 800-63-3] provides guidance on digital identities.

Derived Security Requirements

3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.[24] [25]

DISCUSSION

Multifactor authentication requires the use of two or more different factors to authenticate. The factors are defined as something you know (e.g., password, personal identification number [PIN]); something you have (e.g., cryptographic identification device, token); or something you are (e.g., biometric). Multifactor authentication solutions that feature physical authenticators include hardware authenticators providing time-based or challenge-response authenticators and smart cards. In addition to authenticating users at the system level (i.e., at logon), organizations may also employ authentication mechanisms at the application level, when necessary, to provide increased information security.

Access to organizational systems is defined as local access or network access. Local access is any access to organizational systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks. The use of encrypted virtual private networks for connections between organization-controlled and non-organization controlled endpoints may be treated as internal networks with regard to protecting the confidentiality of information.

[24] *Multifactor authentication* requires two or more different factors to achieve authentication. The factors include: something you know (e.g., password/PIN); something you have (e.g., cryptographic identification device, token); or 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.

[25] *Local access* is any access to a 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 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).

[SP 800-63-3] provides guidance on digital identities.

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

DISCUSSION

Authentication processes resist replay attacks if it is impractical to successfully authenticate by recording or replaying previous authentication messages. Replay-resistant techniques include protocols that use nonces or challenges such as time synchronous or challenge-response one-time authenticators.

[SP 800-63-3] provides guidance on digital identities.

3.5.5 Prevent reuse of identifiers for a defined period.

DISCUSSION

Identifiers are provided for users, processes acting on behalf of users, or devices (3.5.1). Preventing reuse of identifiers implies preventing the assignment of previously used individual, group, role, or device identifiers to different individuals, groups, roles, or devices.

3.5.6 Disable identifiers after a defined period of inactivity.

DISCUSSION

Inactive identifiers pose a risk to organizational information because attackers may exploit an inactive identifier to gain undetected access to organizational devices. The owners of the inactive accounts may not notice if unauthorized access to the account has been obtained.

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

DISCUSSION

This requirement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are used as part of multifactor authenticators. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords.

3.5.8 Prohibit password reuse for a specified number of generations.

DISCUSSION

Password lifetime restrictions do not apply to temporary passwords.

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

DISCUSSION

Changing temporary passwords to permanent passwords immediately after system logon ensures that the necessary strength of the authentication mechanism is implemented at the earliest opportunity, reducing the susceptibility to authenticator compromises.

3.5.10 Store and transmit only cryptographically-protected passwords.

DISCUSSION

Cryptographically-protected passwords use salted one-way cryptographic hashes of passwords. See [NIST CRYPTO].

3.5.11 Obscure feedback of authentication information.

DISCUSSION

The feedback from systems does not provide any information that would allow unauthorized individuals to compromise authentication mechanisms. For some types of systems or system components, for example, desktop or notebook computers with relatively large monitors, the threat (often referred to as shoulder surfing) may be significant. For other types of systems or components, for example, mobile devices with small displays, this threat may be less significant, and is balanced against the increased likelihood of typographic input errors due to the small keyboards. Therefore, the means for obscuring the authenticator feedback is selected accordingly. Obscuring authenticator feedback includes displaying asterisks when users type passwords into input devices or displaying feedback for a very limited time before fully obscuring it.

3.6 INCIDENT RESPONSE

Basic Security Requirements

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

DISCUSSION

Organizations recognize that incident handling capability is dependent on the capabilities of organizational systems and the mission/business processes being supported by those systems. Organizations consider incident handling as part of the definition, design, and development of mission/business processes and systems. Incident-related information can be obtained from a variety of sources including audit monitoring, network monitoring, physical access monitoring, user and administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including mission/business owners, system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive.

As part of user response activities, incident response training is provided by organizations and is linked directly to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the system; system administrators may require additional training on how to handle or remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification/reporting of suspicious activities from external and internal sources. User response activities also includes incident response assistance which may consist of help desk support, assistance groups, and access to forensics services or consumer redress services, when required.

[SP 800-61] provides guidance on incident handling. [SP 800-86] and [SP 800-101] provide guidance on integrating forensic techniques into incident response. [SP 800-161] provides guidance on supply chain risk management.

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

DISCUSSION

Tracking and documenting system security incidents includes maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Reporting incidents addresses specific incident reporting requirements within an organization and the formal incident reporting requirements for the organization. Suspected security incidents may also be reported and include the receipt of suspicious email communications that can potentially contain malicious code. The types of security incidents reported, the content and timeliness of the reports, and the designated reporting authorities reflect applicable laws, Executive Orders, directives, regulations, and policies.

[SP 800-61] provides guidance on incident handling.

Derived Security Requirements

3.6.3 Test the organizational incident response capability.

DISCUSSION

Organizations test incident response capabilities to determine the effectiveness of the capabilities and to identify potential weaknesses or deficiencies. Incident response testing includes the use of checklists, walk-through or tabletop exercises, simulations (both parallel and full interrupt), and comprehensive exercises. Incident response testing can also include a determination of the effects on organizational operations (e.g., reduction in mission capabilities), organizational assets, and individuals due to incident response.

[SP 800-84] provides guidance on testing programs for information technology capabilities.

3.7 MAINTENANCE

Basic Security Requirements

3.7.1 Perform maintenance on organizational systems.[26]

DISCUSSION

This requirement addresses the information security aspects of the system maintenance program and applies to all types of maintenance to any system component (including hardware, firmware, applications) conducted by any local or nonlocal entity. System maintenance also includes those components not directly associated with information processing and data or information retention such as scanners, copiers, and printers.

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

DISCUSSION

This requirement addresses security-related issues with maintenance tools that are not within the organizational system boundaries that process, store, or transmit CUI, but are used specifically for diagnostic and repair actions on those systems. Organizations have flexibility in determining the

[26] 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.

controls in place for maintenance tools, but can include approving, controlling, and monitoring the use of such tools. Maintenance tools are potential vehicles for transporting malicious code, either intentionally or unintentionally, into a facility and into organizational systems. Maintenance tools can include hardware, software, and firmware items, for example, hardware and software diagnostic test equipment and hardware and software packet sniffers.

Derived Security Requirements

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

DISCUSSION

This requirement addresses the information security aspects of system maintenance that are performed off-site and applies to all types of maintenance to any system component (including applications) conducted by a local or nonlocal entity (e.g., in-contract, warranty, in- house, software maintenance agreement).

[SP 800-88] provides guidance on media sanitization.

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

DISCUSSION

If, upon inspection of media containing maintenance diagnostic and test programs, organizations determine that the media contain malicious code, the incident is handled consistent with incident handling policies and procedures.

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

DISCUSSION

Nonlocal maintenance and diagnostic activities are those activities conducted by individuals communicating through an external network. The authentication techniques employed in the establishment of these nonlocal maintenance and diagnostic sessions reflect the network access requirements in 3.5.3.

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

DISCUSSION

This requirement applies to individuals who are performing hardware or software maintenance on organizational systems, while 3.10.1 addresses physical access for individuals whose maintenance duties place them within the physical protection perimeter of the systems (e.g., custodial staff, physical plant maintenance personnel). Individuals not previously identified as authorized maintenance personnel, such as information technology manufacturers, vendors, consultants, and systems integrators, may require privileged access to organizational systems, for example, when required to conduct maintenance activities with little or no notice. Organizations may choose to issue temporary credentials to these individuals based on organizational risk assessments. Temporary credentials may be for one-time use or for very limited time periods.

3.8 MEDIA PROTECTION

Basic Security Requirements

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

DISCUSSION

System media includes digital and non-digital media. Digital media includes diskettes, magnetic tapes, external and removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes paper and microfilm. Protecting digital media includes limiting access to design specifications stored on compact disks or flash drives in the media library to the project leader and any individuals on the development team. Physically controlling system media includes conducting inventories, maintaining accountability for stored media, and ensuring procedures are in place to allow individuals to check out and return media to the media library. Secure storage includes a locked drawer, desk, or cabinet, or a controlled media library.

Access to CUI on system media can be limited by physically controlling such media, which includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return media to the media library, and maintaining accountability for all stored media.

[SP 800-111] provides guidance on storage encryption technologies for end user devices.

3.8.2 **Limit access to CUI on system media to authorized users.**

DISCUSSION

Access can be limited by physically controlling system media and secure storage areas. Physically controlling system media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return system media to the media library, and maintaining accountability for all stored media. Secure storage includes a locked drawer, desk, or cabinet, or a controlled media library.

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

DISCUSSION

This requirement applies to all system media, digital and non-digital, subject to disposal or reuse. Examples include: digital media found in workstations, network components, scanners, copiers, printers, notebook computers, and mobile devices; and non-digital media such as paper and microfilm. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is released for reuse or disposal.

Organizations determine the appropriate sanitization methods, recognizing that destruction may be necessary when other methods cannot be applied to the media requiring sanitization. Organizations use discretion on the employment of sanitization techniques and procedures for media containing information that is in the public domain or publicly releasable or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes destruction, removing CUI from documents, or redacting selected sections or words from a document by obscuring the redacted sections or words in a manner equivalent in effectiveness to removing the words or sections from the document. NARA policy and guidance control sanitization processes for controlled unclassified information.

[SP 800-88] provides guidance on media sanitization.

Derived Security Requirements

3.8.4 Mark media with necessary CUI markings and distribution limitations.[27]

DISCUSSION

The term security marking refers to the application or use of human-readable security attributes. System media includes digital and non-digital media. Marking of system media reflects applicable federal laws, Executive Orders, directives, policies, and regulations. See [NARA MARK].

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

DISCUSSION

Controlled areas are areas or spaces for which organizations provide physical or procedural controls to meet the requirements established for protecting systems and information. Controls to maintain accountability for media during transport include locked containers and cryptography. Cryptographic mechanisms can provide confidentiality and integrity protections depending upon the mechanisms used. Activities associated with transport include the actual transport as well as those activities such as releasing media for transport and ensuring that media enters the appropriate transport processes. For the actual transport, authorized transport and courier personnel may include individuals external to the organization. Maintaining accountability of media during transport includes restricting transport activities to authorized personnel and tracking and obtaining explicit records of transport activities as the media moves through the transportation system to prevent and detect loss, destruction, or tampering.

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.

DISCUSSION

This requirement applies to portable storage devices (e.g., USB memory sticks, digital video disks, compact disks, external or removable hard disk drives). See [NIST CRYPTO].

[SP 800-111] provides guidance on storage encryption technologies for end user devices.

3.8.7 Control the use of removable media on system components.

DISCUSSION

In contrast to requirement 3.8.1, which restricts user access to media, this requirement restricts the use of certain types of media on systems, for example, restricting or prohibiting the use of flash drives or external hard disk drives. Organizations can employ technical and nontechnical controls (e.g., policies, procedures, and rules of behavior) to control the use of system media. Organizations may control the use of portable storage devices, for example, by using physical cages on workstations to prohibit access to certain external ports, or disabling or removing the ability to insert, read, or write to such devices.

Organizations may also limit the use of portable storage devices to only approved devices including devices provided by the organization, devices provided by other approved organizations, and devices that are not personally owned. Finally, organizations may control the use of portable

[27] The implementation of this requirement is per marking guidance in [32 CFR 2002] and [NARA CUI]. Standard Form (SF) 902 (approximate size 2.125" x 1.25") and SF 903 (approximate size 2.125" x .625") can be used on media that contains CUI such as hard drives, or USB devices. Both forms are available from https://www.gsaadvantage.gov. SF 902: NSN 7540-01-679-3318. SF 903: NSN 7540-01-679-3319.

storage devices based on the type of device, prohibiting the use of writeable, portable devices, and implementing this restriction by disabling or removing the capability to write to such devices.

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

DISCUSSION

Requiring identifiable owners (e.g., individuals, organizations, or projects) for portable storage devices reduces the overall risk of using such technologies by allowing organizations to assign responsibility and accountability for addressing known vulnerabilities in the devices (e.g., insertion of malicious code).

3.8.9 Protect the confidentiality of backup CUI at storage locations.

DISCUSSION

Organizations can employ cryptographic mechanisms or alternative physical controls to protect the confidentiality of backup information at designated storage locations. Backed-up information containing CUI may include system-level information and user-level information. System-level information includes system-state information, operating system software, application software, and licenses. User-level information includes information other than system-level information.

3.9 PERSONNEL SECURITY

Basic Security Requirements

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

DISCUSSION

Personnel security screening (vetting) activities involve the evaluation/assessment of individual's conduct, integrity, judgment, loyalty, reliability, and stability (i.e., the trustworthiness of the individual) prior to authorizing access to organizational systems containing CUI. The screening activities reflect applicable federal laws, Executive Orders, directives, policies, regulations, and specific criteria established for the level of access required for assigned positions.

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

DISCUSSION

Protecting CUI during and after personnel actions may include returning system-related property and conducting exit interviews. System-related property includes hardware authentication tokens, identification cards, system administration technical manuals, keys, and building passes. Exit interviews ensure that individuals who have been terminated understand the security constraints imposed by being former employees and that proper accountability is achieved for system-related property. Security topics of interest at exit interviews can include reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and non-availability of supervisors. For termination actions, timely execution is essential for individuals terminated for cause. In certain situations, organizations consider disabling the system accounts of individuals that are being terminated prior to the individuals being notified.

This requirement applies to reassignments or transfers of individuals when the personnel action is permanent or of such extended durations as to require protection. Organizations define the CUI protections appropriate for the types of reassignments or transfers, whether permanent or extended. Protections that may be required for transfers or reassignments to other positions

within organizations include returning old and issuing new keys, identification cards, and building passes; changing system access authorizations (i.e., privileges); closing system accounts and establishing new accounts; and providing for access to official records to which individuals had access at previous work locations and in previous system accounts.

Derived Security Requirements

None.

3.10 PHYSICAL PROTECTION

Basic Security Requirements

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

DISCUSSION

This requirement applies to employees, individuals with permanent physical access authorization credentials, and visitors. Authorized individuals have credentials that include badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, directives, policies, regulations, standards, procedures, and guidelines. This requirement applies only to areas within facilities that have not been designated as publicly accessible.

Limiting physical access to equipment may include placing equipment in locked rooms or other secured areas and allowing access to authorized individuals only; and placing equipment in locations that can be monitored by organizational personnel. Computing devices, external disk drives, networking devices, monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of equipment.

3.10.2 **Protect and monitor the physical facility and support infrastructure for organizational systems.**

DISCUSSION

Monitoring of physical access includes publicly accessible areas within organizational facilities. This can be accomplished, for example, by the employment of guards; the use of sensor devices; or the use of video surveillance equipment such as cameras. Examples of support infrastructure include system distribution, transmission, and power lines. Security controls applied to the support infrastructure prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Physical access controls to support infrastructure include locked wiring closets; disconnected or locked spare jacks; protection of cabling by conduit or cable trays; and wiretapping sensors.

Derived Security Requirements

3.10.3 **Escort visitors and monitor visitor activity.**

DISCUSSION

Individuals with permanent physical access authorization credentials are not considered visitors. Audit logs can be used to monitor visitor activity.

3.10.4 **Maintain audit logs of physical access.**

DISCUSSION

Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to systems or system components requiring supplemental access controls, or both. System components (e.g., workstations, notebook computers) may be in areas designated as publicly accessible with organizations safeguarding access to such devices.

3.10.5 **Control and manage physical access devices.**

DISCUSSION

Physical access devices include keys, locks, combinations, and card readers.

3.10.6 **Enforce safeguarding measures for CUI at alternate work sites.**

DISCUSSION

Alternate work sites may include government facilities or the private residences of employees. Organizations may define different security requirements for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites.

[SP 800-46] and [SP 800-114] provide guidance on enterprise and user security when teleworking.

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 systems and the associated processing, storage, or transmission of CUI.**

DISCUSSION

Clearly defined system boundaries are a prerequisite for effective risk assessments. Such risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations, organizational assets, and individuals based on the operation and use of organizational systems. Risk assessments also consider risk from external parties (e.g., service providers, contractors operating systems on behalf of the organization, individuals accessing organizational systems, outsourcing entities). Risk assessments, either formal or informal, can be conducted at the organization level, the mission or business process level, or the system level, and at any phase in the system development life cycle.

[SP 800-30] provides guidance on conducting risk assessments.

Derived Security Requirements

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

DISCUSSION

Organizations determine the required vulnerability scanning for all system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. The vulnerabilities to be scanned are readily updated as new vulnerabilities are discovered, announced, and scanning methods developed. This process ensures that potential vulnerabilities in the system are identified and addressed as quickly as possible. Vulnerability analyses for custom software applications may require additional approaches such as static

analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in source code reviews and in a variety of tools (e.g., static analysis tools, web-based application scanners, binary analyzers) and in source code reviews. Vulnerability scanning includes: scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for improperly configured or incorrectly operating information flow control mechanisms.

To facilitate interoperability, organizations consider using products that are Security Content Automated Protocol (SCAP)-validated, scanning tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention, and that employ the Open Vulnerability Assessment Language (OVAL) to determine the presence of system vulnerabilities. Sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD).

Security assessments, such as red team exercises, provide additional sources of potential vulnerabilities for which to scan. Organizations also consider using scanning tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS). In certain situations, the nature of the vulnerability scanning may be more intrusive or the system component that is the subject of the scanning may contain highly sensitive information. Privileged access authorization to selected system components facilitates thorough vulnerability scanning and protects the sensitive nature of such scanning.

[SP 800-40] provides guidance on vulnerability management.

3.11.3 Remediate vulnerabilities in accordance with risk assessments.

DISCUSSION

Vulnerabilities discovered, for example, via the scanning conducted in response to 3.11.2, are remediated with consideration of the related assessment of risk. The consideration of risk influences the prioritization of remediation efforts and the level of effort to be expended in the remediation for specific vulnerabilities.

3.12 SECURITY ASSESSMENT

Basic Security Requirements

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

DISCUSSION

Organizations assess security controls in organizational systems and the environments in which those systems operate as part of the system development life cycle. Security controls are the safeguards or countermeasures organizations implement to satisfy security requirements. By assessing the implemented security controls, organizations determine if the security safeguards or countermeasures are in place and operating as intended. Security control assessments ensure that information security is built into organizational systems; identify weaknesses and deficiencies early in the development process; provide essential information needed to make risk-based decisions; and ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls as documented in system security plans.

Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted.

Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Organizations can choose to use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of systems during the system life cycle.

[SP 800-53] provides guidance on security and privacy controls for systems and organizations. [SP 800-53A] provides guidance on developing security assessment plans and conducting assessments.

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

DISCUSSION

The plan of action is a key document in the information security program. Organizations develop plans of action that describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented. Organizations can document the system security plan and plan of action as separate or combined documents and in any chosen format.

Federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the nonfederal organization. [NIST CUI] provides supplemental material for Special Publication 800-171 including templates for plans of action.

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

DISCUSSION

Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess and analyze security controls and information security-related risks at a frequency sufficient to support risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Providing access to security information on a continuing basis through reports or dashboards gives organizational officials the capability to make effective and timely risk management decisions.

Automation supports more frequent updates to hardware, software, firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Monitoring requirements, including the need for specific monitoring, may also be referenced in other requirements.

[SP 800-137] provides guidance on continuous monitoring.

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.[28]

DISCUSSION

System security plans relate security requirements to a set of security controls. System security plans also describe, at a high level, how the security controls meet those security requirements, but do not provide detailed, technical descriptions of the design or implementation of the controls.

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

System security plans contain sufficient information to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk if the plan is implemented as intended. Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition.

Federal agencies may consider the submitted system security plans and plans of action as critical inputs to an overall risk management decision to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the nonfederal organization.

[SP 800-18] provides guidance on developing security plans. [NIST CUI] provides supplemental material for Special Publication 800-171 including templates for system security plans.

Derived Security Requirements

None.

3.13 SYSTEM AND COMMUNICATIONS PROTECTION

Basic Security Requirements

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

DISCUSSION

Communications can be monitored, controlled, and protected at boundary components and by restricting or prohibiting interfaces in organizational systems. Boundary components include gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a system security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Restricting or prohibiting interfaces in organizational systems includes restricting external web communications traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses.

Organizations consider the shared nature of commercial telecommunications services in the implementation of security requirements associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions.

[SP 800-41] provides guidance on firewalls and firewall policy. [SP 800-125B] provides guidance on security for virtualization technologies.

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

DISCUSSION

Organizations apply systems security engineering principles to new development systems or systems undergoing major upgrades. For legacy systems, organizations apply systems security

engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware components within those systems. The application of systems security engineering concepts and principles helps to develop trustworthy, secure, and resilient systems and system components and reduce the susceptibility of organizations to disruptions, hazards, and threats. Examples of these concepts and principles include developing layered protections; establishing security policies, architecture, and controls as the foundation for design; incorporating security requirements into the system development life cycle; delineating physical and logical security boundaries; ensuring that developers are trained on how to build secure software; and performing threat modeling to identify use cases, threat agents, attack vectors and patterns, design patterns, and compensating controls needed to mitigate risk. Organizations that apply security engineering concepts and principles can facilitate the development of trustworthy, secure systems, system components, and system services; reduce risk to acceptable levels; and make informed risk-management decisions.

[SP 800-160-1] provides guidance on systems security engineering.

Derived Security Requirements

3.13.3 Separate user functionality from system management functionality.

DISCUSSION

System management functionality includes functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from system management functionality is physical or logical. Organizations can implement separation of system management functionality from user functionality by using different computers, different central processing units, different instances of operating systems, or different network addresses; virtualization techniques; or combinations of these or other methods, as appropriate. This type of separation includes web administrative interfaces that use separate authentication methods for users of any other system resources. Separation of system and user functionality may include isolating administrative interfaces on different domains and with additional access controls.

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

DISCUSSION

The control of information in shared system resources (e.g., registers, cache memory, main memory, hard disks) is also commonly referred to as object reuse and residual information protection. This requirement prevents information produced by the actions of prior users or roles (or the actions of processes acting on behalf of prior users or roles) from being available to any current users or roles (or current processes acting on behalf of current users or roles) that obtain access to shared system resources after those resources have been released back to the system. This requirement also applies to encrypted representations of information. This requirement does not address information remanence, which refers to residual representation of data that has been nominally deleted; covert channels (including storage or timing channels) where shared resources are manipulated to violate information flow restrictions; or components within systems for which there are only single users or roles.

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

DISCUSSION

Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones (DMZs). DMZs are typically implemented with boundary control devices and techniques that include routers, gateways, firewalls, virtualization, or cloud-based technologies.

[SP 800-41] provides guidance on firewalls and firewall policy. [SP 800-125B] provides guidance on security for virtualization technologies.

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

DISCUSSION

This requirement applies to inbound and outbound network communications traffic at the system boundary and at identified points within the system. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.

3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

DISCUSSION

Split tunneling might be desirable by remote users to communicate with local system resources such as printers or file servers. However, split tunneling allows unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational information. This requirement is implemented in remote devices (e.g., notebook computers, smart phones, and tablets) through configuration settings to disable split tunneling in those devices, and by preventing configuration settings from being readily configurable by users. This requirement is implemented in the system by the detection of split tunneling (or of configuration settings that allow split tunneling) in the remote device, and by prohibiting the connection if the remote device is using split tunneling.

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

DISCUSSION

This requirement applies to internal and external networks and any system components that can transmit information including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, and facsimile machines. Communication paths outside the physical protection of controlled boundaries are susceptible to both interception and modification. Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of the controls for transmission confidentiality. In such situations, organizations determine what types of confidentiality services are available in commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary safeguards and assurances of the effectiveness of the safeguards through appropriate contracting vehicles, organizations implement compensating safeguards or explicitly accept the additional risk. An example of an alternative physical safeguard is a protected distribution system (PDS) where the distribution medium is protected against electronic or physical intercept, thereby ensuring the confidentiality of the information being transmitted. See [NIST CRYPTO].

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

DISCUSSION

This requirement applies to internal and external networks. Terminating network connections associated with communications sessions include de-allocating associated TCP/IP address or port

pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. Time periods of user inactivity may be established by organizations and include time periods by type of network access or for specific network accesses.

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

DISCUSSION

Cryptographic key management and establishment can be performed using manual procedures or mechanisms supported by manual procedures. Organizations define key management requirements in accordance with applicable federal laws, Executive Orders, policies, directives, regulations, and standards specifying appropriate options, levels, and parameters.

[SP 800-56A] and [SP 800-57-1] provide guidance on cryptographic key management and key establishment.

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

DISCUSSION

Cryptography can be employed to support many security solutions including the protection of controlled unclassified information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals. Cryptography can also be used to support random number generation and hash generation. Cryptographic standards include FIPS-validated cryptography and/or NSA-approved cryptography. See [NIST CRYPTO]; [NIST CAVP]; and [NIST CMVP].

3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.[29]

DISCUSSION

Collaborative computing devices include networked white boards, cameras, and microphones. Indication of use includes signals to users when collaborative computing devices are activated. 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.

3.13.13 Control and monitor the use of mobile code.

DISCUSSION

Mobile code technologies include Java, JavaScript, ActiveX, Postscript, PDF, Flash animations, and VBScript. Decisions regarding the use of mobile code in organizational systems are based on the potential for the code to cause damage to the systems if used maliciously. Usage restrictions and implementation guidance apply to the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations, notebook computers, and devices (e.g., smart phones). Mobile code policy and procedures address controlling or preventing the development, acquisition, or introduction of unacceptable mobile code in systems, including requiring mobile code to be digitally signed by a trusted source.

[29] 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.

[SP 800-28] provides guidance on mobile code.

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

DISCUSSION

VoIP has different requirements, features, functionality, availability, and service limitations when compared with the Plain Old Telephone Service (POTS) (i.e., the standard telephone service). In contrast, other telephone services are based on high-speed, digital communications lines, such as Integrated Services Digital Network (ISDN) and Fiber Distributed Data Interface (FDDI). The main distinctions between POTS and non-POTS services are speed and bandwidth. To address the threats associated with VoIP, usage restrictions and implementation guidelines are based on the potential for the VoIP technology to cause damage to the system if it is used maliciously. Threats to VoIP are similar to those inherent with any Internet-based application.

[SP 800-58] provides guidance on Voice Over IP Systems.

3.13.15 Protect the authenticity of communications sessions.

DISCUSSION

Authenticity protection includes protecting against man-in-the-middle attacks, session hijacking, and the insertion of false information into communications sessions. This requirement addresses communications protection at the session versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted.

[SP 800-77], [SP 800-95], and [SP 800-113] provide guidance on secure communications sessions.

3.13.16 Protect the confidentiality of CUI at rest.

DISCUSSION

Information at rest refers to the state of information when it is not in process or in transit and is located on storage devices as specific components of systems. The focus of protection at rest is not on the type of storage device or the frequency of access but rather the state of the information. Organizations can use different mechanisms to achieve confidentiality protections, including the use of cryptographic mechanisms and file share scanning. Organizations may also use other controls including secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved or continuous monitoring to identify malicious code at rest. See [NIST CRYPTO].

3.14 SYSTEM AND INFORMATION INTEGRITY

Basic Security Requirements

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

DISCUSSION

Organizations identify systems that are affected by announced software and firmware flaws including potential vulnerabilities resulting from those flaws and report this information to designated personnel with information security responsibilities. Security-relevant updates include patches, service packs, hot fixes, and anti-virus signatures. Organizations address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations can take advantage of available resources such as the Common Weakness

Enumeration (CWE) database or Common Vulnerabilities and Exposures (CVE) database in remediating flaws discovered in organizational systems.

Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types of remediation.

[SP 800-40] provides guidance on patch management technologies.

3.14.2 Provide protection from malicious code at designated locations within organizational systems.

DISCUSSION

Designated locations include system entry and exit points which may include firewalls, remote-access servers, workstations, electronic mail servers, web servers, proxy servers, notebook computers, and mobile devices. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways including web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities.

Malicious code protection mechanisms include anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended.

[SP 800-83] provides guidance on malware incident prevention.

3.14.3 Monitor system security alerts and advisories and take action in response.

DISCUSSION

There are many publicly available sources of system security alerts and advisories. For example, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) generates security alerts and advisories to maintain situational awareness across the federal government and in nonfederal organizations. Software vendors, subscription services, and industry information sharing and analysis centers (ISACs) may also provide security alerts and advisories. Examples of response actions include notifying relevant external organizations, for example, external mission/business partners, supply chain partners, external service providers, and peer or supporting organizations

[SP 800-161] provides guidance on supply chain risk management.

Derived Security Requirements

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

DISCUSSION

Malicious code protection mechanisms include anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include logic bombs, back doors, and other types of cyber-attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended.

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

DISCUSSION

Periodic scans of organizational systems and real-time scans of files from external sources can detect malicious code. Malicious code can be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using techniques such as steganography. Malicious code can be inserted into systems in a variety of ways including web accesses, electronic mail, electronic mail attachments, and portable storage devices. Malicious code insertions occur through the exploitation of system vulnerabilities.

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

DISCUSSION

System monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system. Organizations can monitor systems, for example, by observing audit record activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. System monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include selected perimeter locations and near server farms supporting critical applications, with such devices being employed at managed system interfaces. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of systems to support such objectives.

System monitoring is an integral part of continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless.

Unusual or unauthorized activities or conditions related to inbound/outbound communications traffic include internal traffic that indicates the presence of malicious code in systems or propagating among system components, the unauthorized exporting of information, or signaling to external systems. Evidence of malicious code is used to identify potentially compromised

systems or system components. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other requirements.

[SP 800-94] provides guidance on intrusion detection and prevention systems.

3.14.7 Identify unauthorized use of organizational systems.

DISCUSSION

System monitoring includes external and internal monitoring. System monitoring can detect unauthorized use of organizational systems. System monitoring is an integral part of continuous monitoring and incident response programs. Monitoring is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Output from system monitoring serves as input to continuous monitoring and incident response programs.

Unusual/unauthorized activities or conditions related to inbound and outbound communications traffic include internal traffic that indicates the presence of malicious code in systems or propagating among system components, the unauthorized exporting of information, or signaling to external systems. Evidence of malicious code is used to identify potentially compromised systems or system components. System monitoring requirements, including the need for specific types of system monitoring, may be referenced in other requirements.

[SP 800-94] provides guidance on intrusion detection and prevention systems.