November 6, 2018

DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented

This guidance was developed to facilitate the consistent review of how the System Security Plan and associated Plans of Action address the NIST SP 800-171 security requirements, and the impact that the 'not yet implemented' NIST SP 800-171 Security Requirements have on an information system. The guidance is designed to help the program office/requiring activity determine the impact of NIST SP 800-171 security requirements not yet met, and in certain cases, to identify when a contractor may have misinterpreted a requirement (which they actually may meet). The guidance is not to be used to assess implemented security requirements, nor to compare or score a company's approach to implementing a security requirement.

The column "Impact if this requirement is not yet implemented" addresses the potential security consequences if a specific NIST SP 800-171 requirement is not implemented. While for many requirements this may be obvious, for others the actual impact is less clear because the requirement is essential for the implementation of other security requirements. For example, an accurate inventory of software and hardware is necessary in order to know what patches need to be applied.

The column "Implementation" addresses the approach a company might use to implement the NIST SP 800-171 security requirement, such as a policy, process, configuration, software or hardware change, or any combination of these. In many cases, the approach is determined by the size or complexity of the information system. DoD clarifying information is also provided in the implementation column to address requirements which are often over-analyzed and/or misunderstood. If the security requirement is unimplemented, the Requiring Activity might consider a follow-up to ensure the company understands the requirement.

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
3.1 ACCESS CONTROL Access is the ability to make use of any system resource. Access control is the process of granting or denying requests to: use information; use information processing services; and enter company facilities. System-based access controls are called logical access controls. Logical access controls prescribe not only who or what (in the case of a process) is permitted to have access to a system resource, but also the type of access that is permitted. Controlling physical access to company facilities is also important. It provides for the protection of employees, plant equipment, hardware, software, networks, and data from physical actions and events that could cause serious loss or damage to the company.		
3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	Failure to limit system use to authorized users, processes or devices puts the security of the system at extreme risk, increases the likelihood of unauthorized access and loss of CUI.	METHOD(S)(S) TO IMPLEMENT: IT Configuration
3.1.2 Limit system access to the types of transactions and functions that authorized users are permitted to execute.	Failure to limit system access to transactions and functions authorized users are permitted to execute puts the security of the system at extreme risk, increases the likelihood of unauthorized access and loss of CUI.	METHOD(S) TO IMPLEMENT: IT Configuration
3.1.3 Control the flow of CUI in accordance with approved authorizations.	Failure to define and control where CUI can flow (i.e., between system components) can result in unauthorized access to or exposure of CUI.	METHOD(S) TO IMPLEMENT: IT Configuration The solutions may include firewalls, proxies, encryption, and other security technologies.
3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	Failure to separate duties may result in a single individual being able to conduct unauthorized activities alone, without having to involve other individuals, thus increasing the security risk to the system and the likelihood of unauthorized access to CUI.	METHOD(S) TO IMPLEMENT: IT Configuration
3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.	Failure to apply the principle of least privilege may result in a single individual being able to conduct unauthorized or inappropriate activities – including those which directly affect the security state of the system, thus increasing the security risk to the system and the likelihood of unauthorized access to CUI.	METHOD(S) TO IMPLEMENT: IT Configuration

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
3.1.6 Use non-privileged accounts or roles when accessing non-security functions.	Use of privileged accounts for non-privileged functions (e.g., checking e-mail, browsing the Internet) increases the exposure of the privileged role to malicious activity.	METHOD(S) TO IMPLEMENT: IT Configuration When all regular users have limited administrative privileges (e.g., to load software), they are not considered privileged users.
3.1.7 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Allowing non-privileged users to execute privileged functions defeats the purpose of least privilege and puts the system's security at risk both to insider and external threats. Failure to audit execution of privilege functions puts the systems security at risk of unauthorized or inappropriate activity by the privileged user.	METHOD(S) TO IMPLEMENT: IT Configuration IMPLEMENTATION NOTES: • When all regular users have limited administrative privileges (e.g., to load software), they are not considered privileged users, and do not require auditing as privileged users.
3.1.8 Limit unsuccessful logon attempts.	Failure to limit unsuccessful logon attempts makes the system susceptible to brute force attacks.	METHOD(S) TO IMPLEMENT: IT Configuration
3.1.9 Provide privacy and security notices consistent with applicable CUI rules.	Failure to provide proper notices may result in the unauthorized and inadvertent exposure of particular categories of CUI data, such as Privacy, Export Controlled or Law Enforcement Sensitive information.	METHOD(S) TO IMPLEMENT: IT Configuration IMPLEMENTATION NOTES: • This requirement references the National Archives and Records Administration's (NARA) Federal rule (32 CFR 2002) implementing its CUI program. It would apply if a specific type of CUI (i.e., information that requires safeguarding or dissemination controls pursuant to law, regulation or Government-wide policy) requires such notices (e.g., before accessing or entering the data). This is not common.
3.1.10 Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.	Failure to implement session lock with pattern-hiding displays may allow unauthorized personnel access to the system itself or to view CUI displayed on the screen.	METHOD(S) TO IMPLEMENT: IT Configuration

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
3.1.11 Terminate (automatically) a user session after a defined condition.	Failure to terminate a user session automatically may allow unauthorized access to a session no longer in active use.	METHOD(S) TO IMPLEMENT: IT Configuration
3.1.12 Monitor and control remote access sessions.	Failure to monitor and control remote access sessions puts the information system at high risk for unauthorized use.	METHOD(S) TO IMPLEMENT: Hardware
3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	Failure to use cryptographic mechanism to protect the confidentiality of remote access sessions makes the CUI transmitted subject to intercept.	METHOD(S) TO IMPLEMENT: Software IMPLEMENTATION NOTES: • Cryptography used to protect the confidentiality of CUI (or in this case covered defense information) must use FIPS-validated cryptography, which means the cryptographic module has to have been tested and validated to meet FIPS 140-1 or-2 requirements.
3.1.14 Route remote access via managed access control points.	Failure to employ managed access control points means remote access is not actually controlled, and puts the information system at high risk for unauthorized access.	METHOD(S) TO IMPLEMENT: Hardware
3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.	Failure to explicitly authorize any remote execution of privileged commands or access to security-related information puts the information system at extreme risk for unauthorized access and subversion.	METHOD(S) TO IMPLEMENT: IT Configuration
3.1.16 Authorize wireless access prior to allowing such connections.	Failure to authorize wireless connections generally means there is little to no control of wireless connections, and puts the information system at extreme risk for unauthorized access and subversion.	METHOD(S) TO IMPLEMENT: IT Configuration

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
3.1.17 Protect wireless access using authentication and encryption.	Failure to authenticate and encrypt wireless access makes such access susceptible to unauthorized access, and puts the information system at extreme risk for unauthorized access and subversion.	METHOD(S) TO IMPLEMENT: Software IMPLEMENTATION NOTES: • Requirements for cryptography used to protect the confidentiality of CUI (or in this case covered defense information) must use FIPS-validated cryptography, which means the cryptographic module has to have been tested and validated to meet FIPS 140-1 or-2 requirements.
3.1.18 Control connection of mobile devices.	Due to the wide variety and capability of mobile devices, failure to control their connection (what devices can be connected under what conditions), puts the information system at high risk for unauthorized access.	METHOD(S) TO IMPLEMENT: IT Configuration
3.1.19 Encrypt CUI on mobile devices and mobile computing platforms.	Failure to encrypt CUI on mobile devices puts any CUI on the devices at risk for unauthorized access if there is a loss of control of the device.	METHOD(S) TO IMPLEMENT: Software IMPLEMENTATION NOTES: • Requirements for cryptography used to protect the confidentiality of CUI (or in this case covered defense information) must use FIPS-validated cryptography, which means the cryptographic module has to have been tested and validated to meet FIPS 140-1 or-2 requirements.
3.1.20 Verify and control/limit connections to and use of external systems.	Failure to control and limit the connection to and use of external systems (e.g., a support contractor, a business partner system) can increase the risk for unauthorized access to the system and CUI.	METHOD(S) TO IMPLEMENT: Hardware

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
3.1.21 Limit use of portable storage devices on external systems.	Failure to limit use of an organization’s portable storage devices on external systems may result in the exposure of CUI and increase exposure to malicious software via the portable storage device.	METHOD(S) TO IMPLEMENT: Policy/Process IMPLMENTATION NOTES: • This is generally implemented by policy restricting use of the device outside the company (e.g., do not use with hotel computers). No IT configuration, or software/hardware is required, though some devices can be configured to work only when connected to a system to which they can authenticate (this is, however, not a requirement).
3.1.22 Control CUI posted or processed on publicly accessible systems.	Failure to control how CUI is posted or processed on publicly accessible systems may result in the inadvertent exposure of CUI on a public system (e.g., public website).	METHOD(S) TO IMPLEMENT: Policy/Process
3.2 AWARENESS AND TRAINING The purpose of information security awareness, training, and education is to enhance security by raising awareness of the need to protect system resources, developing skills and knowledge so system users can perform their jobs more securely, and building in-depth knowledge as needed to design, implement, or operate security programs for organizations and systems. The company is responsible for making sure that managers and users are aware of the security risks associated with their activities and that employees are trained to carry out their information security-related duties and responsibilities.		
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.	Users who are not trained are not aware of cyber risks and thereby pose a significant risk to the security of a network.	METHOD(S) TO IMPLEMENT: Policy/Process
3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	Inadequately trained system administrators and security personnel present a severe risk to the security of the information system as they can improperly configure the system and so render security protections ineffective.	METHOD(S) TO IMPLEMENT: Policy/Process

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.	Users unaware of the characteristics of the Insider Threat may be unable to detect an active Insider, putting the security of the system and its information at risk.	METHOD(S) TO IMPLEMENT: Policy/Process No cost training available at https://www.cdse.edu/catalog/insider-threat.html
3.3 AUDIT AND ACCOUNTABILITY An audit is an independent review and examination of records and activities to assess the adequacy of system requirements and ensure compliance with established policies and operational procedures. An audit trail is a record of individuals who have accessed a system as well as what operations the user has performed during a given period. Audit trails maintain a record of system activity both by system and application processes and by user activity of systems and applications. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance issues, and flaws in applications. Companies should create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity and ensure that the actions of users can be uniquely traced to those users so they can be held accountable.		
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.	Failure to maintain an adequate audit capability will result in an inability to detect unauthorized/unlawful system activity, putting the information system and its information at a severe risk.	METHOD(S) TO IMPLEMENT: IT Configuration
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.	If the audit system is incapable of tracing actions to individuals, it will not be possible to identify and correct improper or illegal activity on the network.	METHOD(S) TO IMPLEMENT: IT Configuration
3.3.3 Review and update events.	Failure to review and update which event are audited (e.g., which event, how and how often) can result in an inadequate audit capability as new or changed system capabilities may not be audited, putting the system at risk.	METHOD(S) TO IMPLEMENT: IT Configuration
3.3.4 Alert in the event of an audit logging process failure.	Failure to activate alerts of audit logging failures (e.g., audit storage has reached capacity) will result in loss of auditing capabilities and failure to detect other failures or improper activity.	METHOD(S) TO IMPLEMENT: IT Configuration This is typically a standard (default) configuration.

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	Lack of an ability to correlate audit review, analysis, and reporting may result in a failure to properly identify or efficiently investigate or report improper activity.	METHOD(S) TO IMPLEMENT: Policy/Process
3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting.	This capability improves the ability to identify improper activity revealed by audit reports.	METHOD(S) TO IMPLEMENT: Software
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.	Time stamps synchronized with an authoritative source are a requirement for proper analysis of audit results since this insures that various audit results can be properly sequenced, e.g., establish cause and effect, to support investigation.	METHOD(S) TO IMPLEMENT: IT Configuration This is a simple configuration to synchronize with authoritative time source (e.g., NIST Internet time service at https://www.nist.gov/pml/time-and-frequency-division/services/internet-time-service-its?iframe=true&width=95%25&height=95%25) and, for small networks, can be synchronized manually.
3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	Auditing can be rendered ineffective (and actually used to cover-up improper activity) if not properly protected from alteration or deletion.	METHOD(S) TO IMPLEMENT: IT Configuration
3.3.9 Limit management of audit logging functionality to a subset of privileged users.	If personnel who are subject to audit (e.g., privileged users) are allowed to manage audit functionality they are subject to, they can invalidate the audit to hide improper activity, putting the security of system at high risk.	METHOD(S) TO IMPLEMENT: IT Configuration

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
3.4 CONFIGURATION MANAGEMENT Configuration management is a collection of activities focused on establishing and maintaining the integrity of information technology products and systems through the control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the System Development Life Cycle (SDLC). Configuration management consists of determining and documenting the appropriate specific settings for a system, conducting security impact analyses, and managing changes through a change control board. It allows the entire system to be reviewed to help ensure that a change made on one system does not have adverse effects on another system. Companies establish and maintain baseline configurations and inventories of company systems, including hardware, software, firmware, and documentation throughout the respective SDLC and establish and enforce security configuration settings for information technology products employed in company systems.		
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.	Establishing baseline configurations is essential as 'out of the box' default configurations are typically insecure (e.g., Password = password, PIN = 0000) and allow anyone to change the configuration, resulting in a severe risk to the security of the system. Inventories of system hardware, software, firmware, etc.) are essential to proper scanning, patching and configuration of the system.	METHOD(S) TO IMPLEMENT: Policy/Process or Software
3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems.	If security configuration settings are not established and enforced, the overall system will be insecure and at high risk.	METHOD(S) TO IMPLEMENT: IT Configuration or Software
3.4.3 Track, review, approve or disapprove, and log changes to organizational systems.	If changes are not properly managed the system will rapidly fall out of proper configuration, become insecure and at high risk. Additionally, failure to log approved changes makes identifying unauthorized changes made by an intruder, extremely difficult to detect.	METHOD(S) TO IMPLEMENT: Policy/Process
3.4.4 Analyze the security impact of changes prior to implementation.	Failure to analyze the security implications of a change before implementation may result in unintended and severe security consequences.	METHOD(S) TO IMPLEMENT: Policy/Process

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	Failure to impose access restrictions related to changes (e.g., insuring only qualified, authorized personnel can implement changes) can result in unauthorized changes being made (purposely or inadvertently) that result in the system being insecure and at high risk.	METHOD(S) TO IMPLEMENT: IT Configuration
3.4.6 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	Systems should be configured to provide only functions that are needed. Systems with unconstrained or unnecessary functions are inherently more insecure and so susceptible to intrusion or subversion.	METHOD(S) TO IMPLEMENT: IT Configuration
3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	Unneeded but enabled programs, functions, ports, protocols and services can provide ready access for misuse or intrusion (especially since if not needed they typically are not securely configured or monitored).	METHOD(S) TO IMPLEMENT: IT Configuration or Software
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.	Failure to prevent the use of unauthorized software can expose the information system to malicious software, covert channels for exploitation of the system, or compromise of its data.	METHOD(S) TO IMPLEMENT: Policy/Process, IT Configuration, or Software This requirement is to Blacklist OR Whitelist. Blacklist can be a policy and process to prohibit types of software (e.g., games) or non-company software, and enforced by periodic review of software on workstations.

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
3.4.9 Control and monitor user-installed software.	Failure to control the software a user can install may introduce malware and vulnerabilities to the network.	<u>METHOD(S) TO IMPLEMENT</u>: Policy/Process, IT Configuration; Software • This requirement does not necessarily require use of IT configuration or software, although that would be the typical means of implementing. A policy/process of periodic examination of user accounts is acceptable. <u>IMPLEMENTATION NOTES:</u> • This requirement is necessary to protect the overall system processing CUI. It is not about software used to actually process CUI.
3.5 IDENTIFICATION AND AUTHENTICATION For most systems, identification and authentication is often the first line of defense. Identification is the means of verifying the identity of a user, process, or device, typically as a prerequisite for granting access to resources in a system. Identification and authentication is a technical measure that prevents unauthorized individuals or processes from entering a system. Identification and authentication is a critical building block of information security since it is the basis for most types of access control and for establishing user accountability. Access control often requires that the system can identify and differentiate between users. Companies should identify system users, processes acting on behalf of users, or devices and authenticate or verify the identities of those users, processes, or devices, as a prerequisite to allowing access to company systems.		
3.5.1 Identify system users, processes acting on behalf of users, and devices.	If users, devices or processes are not identified, the activity on the system cannot be properly controlled or monitored, placing the security of the system and its information at high risk.	<u>METHOD(S) TO IMPLEMENT</u>: IT Configuration
3.5.2 Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	If identities are not authenticated prior to providing access to the system, then the activities of users, devices, and processes cannot be properly controlled and monitored, placing the security of the system and its information at high risk.	<u>METHOD(S) TO IMPLEMENT</u>: IT Configuration

NIST SP 800-171 Security Requirement		Impact if this requirement is not yet Implemented	Implementation
3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	Failure to use multifactor authentication results in weak authentication, typically via simple passwords, which makes it easier for the intruder to assume the identity of an authorized user or privileged user, and compromise the security of the system and its information.	METHOD(S) TO IMPLEMENT: Hardware/Software IMPLEMENTATION NOTES: • Multifactor authentication (MFA) to an information system uses two or more methods of authentication involving something you know (e.g., password); something you have (e.g., a One-Time Password (OTP) generating device like a fob, smart-card, or a mobile app on a smart-phone); and something you are (e.g., a biometric like a fingerprint or iris). • Where you are, even in a controlled access facility, is not one of these factors and, generally, would be a condition that applied to many and not unique to the individual being authenticated. • Local Access means access to an organizational 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 means 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). • For a NON-PRIVILEGED user, if it's a standalone computer (e.g., a laptop computer), with no network access, the access can be via single factor authentication (SFA) - MFA is not required. However, if used to connect to a LAN, the network access has to be MFA. Typically, organizational desktops are used for network access and so the user has to use MFA to access their network account. For a PRIVILEGED user, even local access (e.g., to the standalone) requires MFA.

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
		• MFA is not required for access to mobile devices such as smartphones or tablets as there is a separate requirement (3.1.19) to encrypt CUI on mobile devices and mobile computing platforms, and typically mobile devices do not support MFA in order to access the device. However, if the mobile device is used to access a Covered Contractor Information System, then the system has to provide the capability for MFA for access by the device, and which would be entered via the device (e.g., use of a OTP device and a password). • The multifactor authentication system is a requirement for local or network access to the information system, which is different from authentication to a specific information system component (e.g., a router) or an application (e.g., database). While many system components and applications now support (and expect) multifactor authentication, it is not a requirement to implement two-factor authentication on specific devices.
3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	Use of non-replay resistant authentication mechanisms make a system susceptible to intruders recording and replaying previous authentication messages, and increases the likelihood of unauthorized access to the system.	METHOD(S) TO IMPLEMENT: IT Configuration or Software or Hardware Replay-resistant techniques include, for example, protocols that use nonces or challenges such as time synchronous or challenge-response one-time authenticators. (3.5.4, Appendix F, NIST SP 800-171). This capability is typically standard in recent Operating Systems.

NIST SP 800-171 Security Requirement		Impact if this requirement is not yet Implemented	Implementation
3.5.5	Prevent reuse of identifiers for a defined period.	This prevents reuse of the Identifiers (e.g., logon name) assigned to an individual, groups, etc., being reassigned to a different individual and group to insure the identifier is associated with only one user/group. If an identifier is reassigned, the new user may be permitted inappropriate access to system resources (e.g., files) allowed to the previous user.	METHOD(S) TO IMPLEMENT: IT Configuration IMPLEMENTATION NOTES: • There are no minimum acceptable values for "a defined period." The values are left to the DoD contractor to determine.
3.5.6	Disable identifiers after a defined period of inactivity.	Failure to disable inactive identifies could enable an intruder to exploit the inactive identifier (and go unnoticed since the account owner may not notice).	METHOD(S) TO IMPLEMENT: IT Configuration
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	Using weak passwords or not changing characters when creating new passwords makes it substantially easier for the intruder to attack the password.	METHOD(S) TO IMPLEMENT: IT Configuration
3.5.8	Prohibit password reuse for a specified number of generations.	Reusing recently expired passwords makes it substantially easier for the intruder to attack or compromise the password.	METHOD(S) TO IMPLEMENT: IT Configuration
3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	Failure to change temporary passwords immediately puts the system at risk since the temporary password is typically more susceptible to attack or compromise, and known to more than a single individual.	METHOD(S) TO IMPLEMENT: IT Configuration

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
3.5.10 Store and transmit only cryptographically-protected passwords.	Failure to properly encrypt passwords in transit or when stored makes all passwords susceptible to intercept or exfiltration and puts the security of the system and its information at high risk.	<u>METHOD(S) TO IMPLEMENT</u>: IT Configuration <u>IMPLEMENTATION NOTES</u>: • The Supplemental Guidance in NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, for the related security control IA-5(1) notes that "Encrypted representations of passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords." Best practice would add a unique "salt" to the password before hashing. This description applies to the use of "cryptographically-protected passwords" in NIST SP 800-171 as well.
3.5.11 Obscure feedback of authentication information.	Failure to obscure authentication information (e.g., passwords) when entered may result in the observation and compromise of the password (e.g., shoulder surfing).	<u>METHOD(S) TO IMPLEMENT</u>: IT Configuration This is typically a default configuration to replace password text with "dots".
3.6 INCIDENT RESPONSE Systems are subject to a wide range of threat events, from corrupted data files to viruses to natural disasters. Vulnerability to some threat events can be lessened by having standard operating procedures that can be followed in the event of an incident. Companies should establish an operational incident handling capability for company systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities and track, document, and report incidents to company management and/or authorities.		
3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	Lack of an operational incident-handling capability can result in a failure to detect an incident (e.g., intrusion) or to properly analyze the impact and respond, which places the system and its information at high risk.	<u>METHOD(S) TO IMPLEMENT</u>: Policy/Process or Software
3.6.2 Track, document, and report incidents to designated officials and/or authorities	Failure to track and report incidents can result in ineffective and inappropriate response, adversely impacting the system.	<u>METHOD(S) TO IMPLEMENT</u>: Policy/Process or Software

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
both internal and external to the organization.		
3.6.3 Test the organizational incident response capability.	Failure to test the incident response capability may result improper response to an actual incident, placing the security of the system at higher risk.	METHOD(S) TO IMPLEMENT: Policy/Process
3.7 MAINTENANCE To keep systems in good working order and to minimize risks from hardware and software failures, it is important that companies establish procedures for systems maintenance. There are many ways a company can address these maintenance requirements. Companies should perform periodic and timely maintenance on company systems and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.		
3.7.1 Perform maintenance on organizational systems.	This refers to information security aspects of the maintenance program – failure to maintain the system (e.g., apply SW updates, revise configuration settings, refresh SW beyond end of life, maintain licenses) can result in significant security vulnerabilities.	METHOD(S) TO IMPLEMENT: Policy/Process
3.7.2 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	Failure to control maintenance can result in the introduction of malicious code, theft of data or creation of ‘back doors’ for future exploitation.	METHOD(S) TO IMPLEMENT: Policy/Process
3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.	Failure to sanitize equipment can result in exposure or loss of CUI.	METHOD(S) TO IMPLEMENT: Policy/Process
3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	Failure to check diagnostic or test media for malicious code can result in the introduction of malicious code into the system, and may result in exfiltration of data or creation of ‘back doors’ for future exploitation.	METHOD(S) TO IMPLEMENT: Software

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	Failure to strongly authenticate remote maintenance sessions can result in unauthorized access to the information system, introduction of malicious code or creation of back doors for future exploitation.	METHOD(S) TO IMPLEMENT: Hardware IMPLEMENTATION NOTES: • If remote maintenance sessions are not allowed or company can 'prohibit' remote maintenance access until MFA capability implemented, this requirement is met. • The multifactor authentication for non-local maintenance is intended for recurring non-local maintenance by organizational personnel rather than episodic non-local maintenance by outside vendors where issuance of such credentials for one-time activities is not efficient and may not be advisable. Nevertheless, presuming the individual performing the repair is known and trusted, it is possible to provide for "one-time" multifactor authentication through the use of a password and a separately provided token (e.g., PIN via text message to a cell phone).
3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.	Failure to properly supervise 'outside' maintenance personnel can result in unauthorized exposure of CUI, theft of CUI, introduction of malicious code or creation of 'back doors' for future exploitation.	METHOD(S) TO IMPLEMENT: Policy/Process
3.8 MEDIA PROTECTION Media protection is a requirement that addresses the defense of system media, which can be described as both digital and non-digital. Media protections can restrict access and make media available to authorized personnel only, apply security labels to sensitive information, and provide instructions on how to remove information from media so that the information cannot be retrieved or reconstructed. Media protections also include physically controlling system media and ensuring accountability, as well as restricting mobile devices capable of storing and carrying information into or outside of restricted areas. Companies should protect system media, both paper and digital, limit access to information on system media to authorized users, and sanitize or destroy system media before disposal or release for reuse.		
3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	Failure to properly protect media can lead to loss/ theft of CUI. It can also allow introduction of malicious code or other alteration of the media	METHOD(S) TO IMPLEMENT: Policy/Process

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
	that can affect the security of the system using the media.	
3.8.2 Limit access to CUI on system media to authorized users.	Failure to limit the access to CUI on system media to authorized users may result in unauthorized exposure of CUI.	METHOD(S) TO IMPLEMENT: Policy/Process IMPLEMENTATION NOTES: • This requirement is meant to be applied by using physical controls to access physical media, but other mechanisms for logical access, such as digital rights management protections or discretionary access control lists, are acceptable.
3.8.3 Sanitize or destroy system media containing CUI before disposal or release for reuse.	Failure to sanitize system media containing CUI prior to disposal or release may result in an unauthorized exposure of CUI.	METHOD(S) TO IMPLEMENT: Software
3.8.4 Mark media with necessary CUI markings and distribution limitations.	Failure to properly mark media containing CUI may result in an unauthorized exposure of CUI.	METHOD(S) TO IMPLEMENT: Policy/Process IMPLEMENTATION NOTES: • This requirement applies to information system media with CUI, which includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. It would not include cell phones. • It is NOT a requirement about marking non-system media (e.g., contract deliverables) with CUI markings. • The requirements of the clause only apply to covered defense information, i.e., information provided or developed by the contractor for DoD which is Controlled Technical Information or other information requiring protection by law, regulation or government-wide policy, that

NIST SP 800-171 Security Requirement		Impact if this requirement is not yet Implemented	Implementation
			is processed, transmitted or stored in the contractor's unclassified information system. It does not apply to information provided by or developed for non-DoD organizations. Guidance on marking media, along with other materials, should be addressed separately in the contract and is derived from DoD Manual 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI).
3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	Failure to control access/maintain accountability of media with CUI during transport may result in unauthorized exposure of CUI.	METHOD(S) TO IMPLEMENT: Policy/Process
3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport outside of controlled areas unless otherwise protected by alternative physical safeguards.	Failure to encrypt media with CUI, if not otherwise protected, could result in the loss and unauthorized exposure of CUI.	METHOD(S) TO IMPLEMENT: Policy/Process or Software. Physical control such as in custody of employees during transport or shipment via commercial carrier – USPS, UPS, FedEx – are examples of "alternative physical safeguards".
3.8.7	Control the use of removable media on system components.	Failure to control of the use of removable media on system components can result in the introduction of malware and/or massive theft/exfiltration of CUI from the system.	METHOD(S) TO IMPLEMENT: IT Configuration A policy and process on allowable use of removable media (e.g., thumb drives, DVDs), including monitoring for compliance, would address this requirement.
3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	Use of portable storage devices of unknown provenance makes introduction of malware into the system a high probability.	METHOD(S) TO IMPLEMENT: Policy/Process A policy prohibiting use of anonymous portable storage devices (e.g., thumb drives) and a process

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
		to check on compliance would address this requirement.
3.8.9 Protect the confidentiality of backup CUI at storage locations.	Failure to protect the confidentiality of CUI in backups at storage locations could result in the undetected compromise, loss, or theft of the CUI.	METHOD(S) TO IMPLEMENT: Policy/Process or Software
3.9 PERSONNEL SECURITY Personnel security seeks to minimize the risk that staff (permanent, temporary, or contractor) pose to company assets through the malicious use or exploitation of their legitimate access to the company's resources. Companies should be vigilant when recruiting and hiring new employees, as well as when an employee transfers or is terminated. Companies should ensure that individuals occupying positions of responsibility within the company (including third-party service providers) are trustworthy and meet established security criteria for those positions, ensure that company information and systems are protected during and after personnel actions such as terminations and transfers, and employ formal sanctions for personnel failing to comply with company security policies and procedures.		
3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI.	Failure to properly screen individuals prior to access to systems containing CUI can result in the inappropriate exposure of CUI (especially CUI with limited dissemination controls).	METHOD(S) TO IMPLEMENT: Policy/Process
3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	Failure to update personnel access following transfers and terminations can result in the inappropriate access/exposure of CUI.	METHOD(S) TO IMPLEMENT: Policy/Process
3.10 PHYSICAL PROTECTION The term physical (and environmental) security refers to measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment. Companies should limit physical access to systems, equipment, and the respective operating environments to authorized individuals, protect the physical plant and support infrastructure for systems, provide supporting utilities for systems, protect systems against environmental hazards, and provide appropriate environmental controls in facilities containing systems.		
3.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	Failure to protect physical access to the information system could result in the unauthorized access to equipment, disclosure or loss of CUI, introduction of malware, etc.	METHOD(S) TO IMPLEMENT: Policy/Process, Software, Hardware IMPLEMENTATION NOTES:

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
		• The purpose of this requirement is to protect the information system/equipment by limiting physical access to the information system equipment to authorized organizational personnel (e.g., employees). Businesses with IT systems that are not in restricted spaces (e.g., distributed within office environment) may meet this requirement through observation/escort procedures.
3.10.2 Protect and monitor the physical facility and support infrastructure for organizational systems.	Failure to protect and monitor the physical facility can result in physical tampering, eavesdropping, monitoring otherwise 'protected' communications and the exposure or loss of CUI.	METHOD(S) TO IMPLEMENT: Policy/Process, Software, Hardware
3.10.3 Escort visitors and monitor visitor activity.	Failure to escort and monitor visitors can result in the unauthorized exposure or loss of CUI and unauthorized access to equipment.	METHOD(S) TO IMPLEMENT: Policy/Process
3.10.4 Maintain audit logs of physical access.	Failure to maintain logs eliminates ability to identify persons who may have inappropriately accessed CUI or equipment.	METHOD(S) TO IMPLEMENT: Policy/Process Audit logs of physical access specifically to IT systems may be impractical for small IT systems not in restricted space while risk is mitigated by increased observation by employees. This requirement can be met by visitor logs.
3.10.5 Control and manage physical access devices.	Failure to control and manage physical access devices can make physical controls / protections ineffective.	METHOD(S) TO IMPLEMENT: Policy/Process This requirement means having control over keys, combinations and similar access control devices.
3.10.6 Enforce safeguarding measures for CUI at alternate work sites.	Failure to provide proper safeguarding for CUI at alternate work sites can result in inappropriate exposure or loss of CUI.	METHOD(S) TO IMPLEMENT: Policy/Process IMPLEMENTATION NOTES: • If you have alternate work sites that will be used to store, process or transmit covered defense information, the same requirements apply (i.e., there is no difference in requirements between the primary and

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
		alternate work sites), although different methods may be used to meet the requirements at the alternate site.
3.11 RISK ASSESSMENT Risk assessments identify and prioritize risks to company operations, assets, employees, and other organizations that may result from the operation of a system. Risk assessments inform company decision makers and support risk responses by identifying: relevant threats to organizations or threats directed through organizations against other organizations, vulnerabilities both internal and external to organizations, impact (i.e., harm) to the company that may occur given the potential for threats exploiting vulnerabilities, and the likelihood that harm will occur. Companies should periodically assess the risk to operations (e.g., mission, functions, image, and reputation), assets, and employees, which may result from the operation of company systems and the associated processing, storage, or transmission of company information.		
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.	Failure to assess risk periodically can result in not addressing emerging or changing threats or vulnerabilities and increased risk to the information system's security and exposure or loss of CUI.	METHOD(S) TO IMPLEMENT: Policy/Process IMPLEMENTATION NOTES: • There is no defined requirement, methodology or period for the risk assessments, nor is a report required. All of these are dependent on the organization, its mission, changes to its systems and environment – this is a periodic assessment of how you operate to insure you understand your risk, which can change over time. Any changes resulting from the assessment would be reflected in implementing plans of action and in the system security plan per 3.12.2 and 3.12.4.
3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	Failure to scan for vulnerabilities in the system will result in unidentified vulnerabilities that can be used to gain unauthorized access to the system, introduction of malware, and exfiltration of CUI.	METHOD(S) TO IMPLEMENT: Software
3.11.3 Remediate vulnerabilities in accordance with risk assessments.	Failure to patch systems will result in vulnerabilities persisting that can be used to gain	METHOD(S) TO IMPLEMENT: IT Configuration

NIST SP 800-171 Security Requirement	**Impact if this requirement is not yet Implemented**	**Implementation**
	unauthorized access to the system, introduction of malware, and exfiltration of CUI.	
3.12 SECURITY ASSESMENT A security requirement assessment is the testing and/or evaluation of the management, operational, and technical security requirements on a system to determine the extent to which the requirements are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The assessment also helps determine if the implemented requirements are the most effective and cost-efficient solution for the function they are intended to serve. Companies should periodically assess the security requirements in company systems to determine if the requirements are effective in their application, develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in company systems, authorize the operation of company systems and any associated system connections, and monitor security requirements on an ongoing basis to ensure the continued effectiveness of the requirements, and document these actions in the System Security Plan.		
3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application	Failure to periodically assess the security controls may result in ineffective controls that can result in unauthorized access to the system, introduction of malware, and exfiltration of CUI.	METHOD(S) TO IMPLEMENT: Policy/Process IMPLEMENTATION NOTES: • There are no minimum acceptable values for "Periodically assess…" The values are left to the DoD contractor to determine. • There is no defined period for security control assessments, nor is there a report required. The organization should define for itself when controls are assessed, which may be based on a time period determined by its needs and/or events, such as a change to the system or its environment.
3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	Failure to develop and implement plans of action can result in deficiencies not being resolved in a timely manner, placing the security of the system at risk.	METHOD(S) TO IMPLEMENT: Policy/Process IMPLEMENTATION NOTES: • Plans of Action are required for requirements that are applicable and not yet implemented, or when there is a deficiency in a requirement. When all requirements are met and no

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
		deficiencies have been identified, no plan of action is required.
3.12.3 Monitor security controls on ongoing basis to ensure the continued effectiveness of the controls.	Failure to monitor the effectiveness of security controls on an ongoing basis may result in ineffective controls that increase risk of unauthorized access to the system, introduction of malware, and exfiltration of CUI.	METHOD(S) TO IMPLEMENT: Policy/Process or Software IMPLEMENTATION NOTES: • There is no defined period for security control monitoring, nor is there a report required. The organization should define for itself how and when controls are monitored, which may be based on a time period determined by its needs and/or certain events, such as a change to the system or environment.
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.	Lack of a current System Security Plan can result in necessary security controls not being applied or misapplied, unanticipated and unsecure connections allowed, and generally may result in an unacceptable security posture, putting the overall security of the system and its information at risk.	METHOD(S) TO IMPLEMENT: Policy/Process IMPLEMENTATION NOTES: • Revision 1 of the NIST SP 800-171 states that when requested by the requiring activity and submitted by contractor, the system security plan and any associated plans of action demonstrate implementation or planned implementation of the security requirements. • Additionally, Revision 1 notes that “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 or not it is advisable to pursue an agreement or contract with the nonfederal organization.”

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
		• Requiring activities may utilize the system security plan and associated plans of action in a variety of ways in the contract formation/administration process in order to obtain the level of security that they require. • Footnote 26 to NIST SP 800-171 Security Requirement 3.12.4 states that, "There is no prescribed format or specified level of detail for system security plans. However, organizations must ensure that the required information in 3.12.4 is appropriately conveyed in those plans." Additionally, Chapter 3 of NIST SP 800-171, Revision 1 states that, "Organizations can document the system security plan and plan of action as separate or combined documents and in any chosen format." • Due to popular request, NIST has posted a sample template for an SSP – associated with the NIST SP 800-171 posting – but notes that there is no prescribed format.
3.13 SYSTEM AND COMMUNICATIONS PROTECTION System and communications protection requirements provide an array of safeguards for the system. Some of the requirements in this family address the confidentiality information at rest and in transit. The protection of confidentiality can be provided by these requirements through physical or logical means. Companies can better safeguard their information by separating user functionality and system management functionality. Providing this type of protection prevents the presentation of system management-related functionality on an interface for non-privileged users. System and communications protection also establishes boundaries that restrict access to publicly accessible information within a system. Using boundary protections, a company can monitor and control communications at external boundaries as well as key internal boundaries within the system.		
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.	Failure to monitor and control communications at external boundaries and key internal boundaries will likely result (and certainly not prevent) unauthorized communications within and outside the system, increasing the probability of	<u>METHOD(S) TO IMPLEMENT</u>: Hardware

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
	unauthorized access or intrusion into the system, introduction of malware, exfiltration of data, etc.	
3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	Failure to employ appropriate architectural designs, SW development techniques or System Engineering can result in an insecure system built from individually 'secure' parts.	METHOD(S) TO IMPLEMENT: Policy/Process
3.13.3 Separate user functionality from system management functionality.	Failure to separate user and system management functionality can result in users being able to access system administration or management functions, putting the system at risk and increasing the access available to intruders.	METHOD(S) TO IMPLEMENT: IT Configuration
3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.	Failure to prevent information transfer via shared resources (e.g., cache memory, shared disks) can result in unauthorized access to CUI.	METHOD(S) TO IMPLEMENT: IT Configuration or Software or Hardware
3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Failure to use subnetworks (e.g., DMZs) to separate publicly accessible components from internal networks can result in the inadvertent exposure of CUI on the publicly accessible component or inappropriate access by unauthorized personnel to the internal network and CUI.	METHOD(S) TO IMPLEMENT: IT Configuration or Software or Hardware The subnetwork, or "DMZ," can be single or dual firewall(s) that separate the internal network from system components connected to external networks (e.g., the Internet).

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	Failure to employ 'deny by default connections' may result in unintentional connections/traffic, put the security of the system at risk and result in the unauthorized exposure/loss of CUI.	METHOD(S) TO IMPLEMENT: IT Configuration or Software or Hardware This is a standard configuration of a firewall, though may require addition of a firewall if none exists. IMPLEMENTATION NOTES: • This requirement can be met if there is a mechanism to implement "deny all, permit by exception" rule within the path between the external network and the CUI information, but if there are internal elements/segments of the information system that do not have the protections in place to process/store CUI, then they would also fall under this provision.
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).	Failure to prevent split tunneling can provide an intruder access to the protected network via the unprotected network connected via the tunnel, putting the security of the system and CUI at risk.	METHOD(S) TO IMPLEMENT: IT Configuration This is a configuration setting on (typically) laptops to prevent split-tunneling when operating remotely (i.e., connecting to a local unprotected resource (e.g., printer) while simultaneously connected remotely to the protected network.
3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	Failure to encrypt CUI during transmission (outside the protected information system) puts the confidentiality of the CUI at risk.	METHOD(S) TO IMPLEMENT: IT Configuration or Software or Hardware IMPLEMENTATION NOTES: • Requirements for cryptography used to protect the confidentiality of CUI (or in this case covered defense information) must use FIPS-validated cryptography, which means the cryptographic module has to have been tested and validated to meet FIPS 140-1 or-2 requirements. • When implementing this requirement, encryption, though preferred, is not required if

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
		using common-carrier provided MPLS, as the MPLS separation provides sufficient protection without encryption. • Transport Layer Security (TLS) protocol can be used to protect CUI during transmission over the Internet. • The current version of TLS (TLS 1.2) is preferred. If earlier versions must be used to interact with certain organizations, the servers shall not support Secure Sockets Layer (SSL) version 3.0 or earlier. For further information see NIST SP 800-52, Rev 1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, April 2014. • Common Carrier telecommunications circuits or Plain Old Telephone Service (POTS) would not normally be considered part of the information system processing CUI. Data traversing Common Carrier systems should be separately encrypted per 3.13.8. Contracts with Common Carriers to provide telecommunications services may include DFARS Clause 252.204-7012, but should not be interpreted to imply the Common Carrier telecommunications systems themselves have to meet the DFARS requirements. Data transmission of CUI transmitted over standard telephone dial-up service (POTS) similarly should be separately encrypted as no protection is expected to be provided by the telephone system. Voice communication of CUI over the telephone is not addressed by NIST SP 800-171 or by DFARS clause 252.204-7012.

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	Failure to terminate communications session at the completion of the session may result in unintended access to the system and data.	METHOD(S) TO IMPLEMENT: IT Configuration
3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems.	Failure to establish and manage cryptographic keys can result in unauthorized access to the system and CUI.	METHOD(S) TO IMPLEMENT: IT Configuration or Software
3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	Failure to use FIPS-validated cryptography is considered by NIST to be the equivalent of not using cryptography (i.e., not encrypting the data) due to the high failure rate during validation testing and therefore any CUI or system depending upon non-FIPS validated cryptography is at risk of exposure.	METHOD(S) TO IMPLEMENT: IT Configuration or Software or Hardware IMPLEMENTATION NOTES: • Requirements for cryptography used to protect the confidentiality of CUI (or in this case covered defense information) must use FIPS-validated cryptography, which means the cryptographic module has to have been tested & validated to meet FIPS 140-1 or-2 requirements. • Simply using an approved algorithm (e.g., FIPS 197 for AES) is not sufficient – the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140. • When an application or device allows a choice (by selecting FIPS-mode or not), then the FIPS-mode has been validated under FIPS 140-2, but the other options (non-FIPS) allow certain operations that would not meet the FIPS requirements. • More information is available at http://csrc.nist.gov/groups/STM/cmvp/ and

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
		http://csrc.nist.gov/groups/STM/cmvp/validation.html • FIPS-validated cryptography is only required to protect CUI, typically when transmitted or stored external to the covered contractor IT system. It is NOT required for all cryptography – which is often used for other purposes within the protected system.
3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	Failure to prevent remote activation of collaborative computing devices (e.g., networked whiteboards, cameras, microphones, etc) can result in the unauthorized disclosure of CUI.	METHOD(S) TO IMPLEMENT: IT Configuration This is typically a configuration option to prevent (turn off) activation by remote users. This is not required for dedicated video conferencing systems which rely on calling party to activate.
3.13.13 Control and monitor the use of mobile code.	Failure to control/monitor mobile code (e.g., Java, JavaScript, ActiveX, Postscript), which can be used maliciously, can result in damage or failure in the security of the system.	METHOD(S) TO IMPLEMENT: IT Configuration or Software or Hardware IMPLEMENTATION NOTES: • This requirement is necessary to protect the overall system processing CUI. It is not about software used to actually process CUI and is not related to mobile devices.
3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	Failure to control and monitor VoIP technologies (treating VoIP as traditional telephone rather than as IP traffic) can result in unauthorized access to the system or exfiltration of CUI.	METHOD(S) TO IMPLEMENT: IT Configuration or Software or Hardware IMPLEMENTATION NOTES: • This requires treating VoIP as IP (e.g., configuring firewalls appropriately). It does NOT require monitoring content of calls. • Even if outsourced, the internal IT system should have protections in place to control

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
		(albeit limited) and monitor VoIP within the system. • If physically or cryptographically isolated from an information system processing CUI, this control would not apply (but it would be prudent to apply the requirement).
3.13.15 Protect the authenticity of communications sessions.	Failure to insure the authenticity of communications sessions can result in the unauthorized loss of CUI and unauthorized access to the information system via man-in the-middle attacks, session hijacking, etc).	METHOD(S) TO IMPLEMENT: IT Configuration This is often a default configuration.
3.13.16 Protect the confidentiality of CUI at rest.	Failure to protect the confidentiality of CUI at rest can result in the unauthorized disclosure of CUI.	METHOD(S) TO IMPLEMENT: IT Configuration or Software IMPLEMENTATION NOTES: • This does NOT require encryption (except for CUI on mobile devices) if the CUI is protected by other means (e.g., physical protection), or if it is within the boundary of the covered contractor information system (e.g., NIST SP 800-171 compliant). • CUI be stored at rest in any non-mobile device or data center, unencrypted, as long as it is protected by other approved logical or physical methods. The mapped NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, control (SC-8), notes that this requirement is to protect the confidentiality of CUI information at rest when it is located on storage devices as specific components of information systems and that "organizations may employ different mechanisms to achieve confidentiality

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
		protection, including the use of cryptographic mechanisms and file share scanning." Thus, encryption is an option, not a requirement.
3.14 SYSTEM AND INFORMATION INTEGRITY Integrity is defined as guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. It is the assertion that data can only be accessed or modified by the authorized employees. System and information integrity provides assurance that the information being accessed has not been meddled with or damaged by an error in the system. Companies should identify, report, and correct information and system flaws in a timely manner, provide protection from malicious code at appropriate locations within company systems, and monitor system security alerts and advisories and respond appropriately.		
3.14.1 Identify, report, and correct system flaws in a timely manner.	Failure to identify and patch system flaws/vulnerabilities in a timely manner makes the system vulnerable to unauthorized access and malicious software and the exfiltration of CUI.	METHOD(S) TO IMPLEMENT: IT Configuration or Software
3.14.2 Provide protection from malicious code at designated locations within organizational systems.	Failure to provide malicious code protection (e.g., Antivirus) makes the system vulnerable to malicious software, exfiltration of CUI, and unauthorized access.	METHOD(S) TO IMPLEMENT: Software
3.14.3 Monitor system security alerts and advisories and take action in response.	Failure to monitor system security alerts and advisories results in security flaws or threats not being addressed and the system more vulnerable to unauthorized access and exfiltration of CUI.	METHOD(S) TO IMPLEMENT: Policy or Software
3.14.4 Update malicious code protection mechanisms when new releases are available.	Failure to update malicious code protections (e.g., Antivirus signatures) makes the system more susceptible to malicious code, unauthorized access and exfiltration of CUI.	METHOD(S) TO IMPLEMENT: IT Configuration

NIST SP 800-171 Security Requirement	Impact if this requirement is not yet Implemented	Implementation
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.	Failure to periodically scan the system and when downloading, opening, executing files, etc., makes the system more susceptible to malicious code, unauthorized access and exfiltration of CUI.	METHOD(S) TO IMPLEMENT: IT Configuration
3.14.6 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Failure to monitor the information system will result in attacks not being detected and increases the likelihood of unauthorized access to the system and exfiltration of CUI.	METHOD(S) TO IMPLEMENT: Software or Hardware
3.14.7 Identify unauthorized use of organizational systems.	Failure to identify unauthorized use of the system will present a severe risk to the information system and unauthorized access to or exfiltration of CUI.	METHOD(S) TO IMPLEMENT: Software or Hardware