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 and understanding of System Security Plans and Plans of Action, and the impact that NIST SP 800-171 Security Requirements that are 'not yet implemented' have on an information system. The guidance is also intended to assist in prioritizing the implementation of security requirements not yet implemented. 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 guidance provides a 'DoD Value' for each of the NIST SP 800-171 security requirements; addresses the method(s) to implement the security requirements; and when applicable, provides clarifying information for security requirements that are frequently misunderstood. The DoD Value is provided to assess the risk that a security requirement left unimplemented has on an information system, to assess the risk of a security requirement with an identified deficiency, and to address the priority for which an unimplemented requirement should be implemented.

Basis for the DoD Value: NIST SP 800-171 security requirements are derived from security controls in NIST SP 800-53 Revision 4. NIST assigns a priority code of P1, P2, or P3 to each of the NIST SP 800-53 security controls. This prioritization informs the community as to the order in which the security controls should be implemented. A P1 security control has a higher priority for implementation than a P2 control, and a P2 control has a higher priority than a P3 control. This recommended sequencing prioritization helps ensure that security controls upon which other controls depend are implemented first, thus enabling organizations to deploy controls in a more structured and timely manner in accordance with available resources. These NIST SP 800-53 priority codes were considered in the calculation of the DoD Implementation Value for corresponding NIST SP 800-171 security requirements.

DoD Values range from 5 − representing the highest impact on the information system, or highest priority to implement, to 1 − representing the lowest impact on the information system, or lowest priority to implement. The DoD Value for NIST SP 800-171 security requirements associated with P1 security controls is typically 5, but may range between 5 and 3. This range allows for discrimination with requirements that consist of multiple elements which may be partially implemented, or with requirements that, if left unimplemented, may introduce lower or more manageable risk in certain situations, such as in businesses with a small or less complex information system. If the DoD Value for a requirement associated with a P1 security control is less than 5, the comment column will address the reason for the difference. The DoD Value for requirements associated with P2 and P3 security controls are assigned DoD Values of 2 and 1 respectively to reflect the lower priority for implementation.

When a NIST SP 800-171 security requirement is derived from more than one NIST SP 800-53 security control, there may be mixed priorities. In these cases, the DoD Value is based on a holistic view of the security requirement. If two values are entered in the DoD Value column, the comments explain when the lower value may be appropriately assigned. When an implemented NIST SP 800-171 security requirement has an identified deficiency, the DoD Value can range from 5 (for severe, widespread deficiencies) to 0 (for minor shortcomings

scored essentially as “implemented”). In a few cases, the DoD Value will differ substantively from the NIST SP 800-53 priority code since the NIST SP 800-171 requirement varies somewhat from the corresponding NIST SP 800-53 security control, and the original basis for prioritization may no longer apply.

Method to Implement: The comment column 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 comment column to address requirements which are often over-analyzed and/or misunderstood. These comments are not considered in the value assignment methodology, but if the security requirement is unimplemented, the Requiring Activity may consider a follow-up to ensure the company understands the requirement.

NIST SP 800-171 Security Requirement		Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171				Table D-2 NIST SP 800-53r4		
3.1 ACCESS CONTROL						
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	AC-2	Account Management	P1	**5**	METHOD(S)(S) TO IMPLEMENT: IT Configuration
		AC-3	Access Enforcement	P1		
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.				**5**	METHOD(S) TO IMPLEMENT: IT Configuration
		AC-17	Remote Access	P1		
3.1.3	Control the flow of CUI in accordance with approved authorizations.	AC-4	Information Flow Enforcement	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration

NIST SP 800-171 Security Requirement		Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171				Table D-2 NIST SP 800-53r4		
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	AC-5	Separation of Duties	P1	**5/3**	METHOD(S) TO IMPLEMENT: IT Configuration VALUE: For businesses with a small number of information technology personnel to separate duties; risk may be assessed at level 3 if company has few IT assets to manage (e.g., small businesses).
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	AC-6	Least Privilege	P1	**5/3**	METHOD(S) TO IMPLEMENT: IT Configuration VALUE: For businesses with a small number of information technology personnel to separate duties; risk may be assessed at level 3 if company has few IT assets to manage.
		AC-6(1)	Least Privilege *Authorize Access to Security Functions*	P1		
		AC-6(5)	Least Privilege *Privileged Accounts*	P1		
3.1.6	Use non-privileged accounts or roles when accessing nonsecurity functions.	AC-6(2)	Least Privilege *Non-Privileged Access for Nonsecurity Functions*	P1	**5**	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 audit the execution of such functions.	AC-6(9)	Least Privilege *Auditing Use of Privileged Functions*	P1	**5**	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, and do not require auditing as privileged users.
		AC-6(10)	Least Privilege *Prohibit Non-Privileged Users from Executing Privileged Functions*	P1		
3.1.8	Limit unsuccessful logon attempts.	AC-7	Unsuccessful Logon Attempts	P2	**2**	METHOD(S) TO IMPLEMENT: IT Configuration

NIST SP 800-171 Security Requirement		Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171				Table D-2 NIST SP 800-53r4		
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	AC-8	System Use Notification	P1	**1**	METHOD(S) TO IMPLEMENT: IT Configuration VALUE: This risk assessment differs from NIST's high priority for AC-8, System Use Notification (i.e., computer banner on acceptable/lawful use). Since the 'System Use Notification' generally is not related to protection of CUI, requirement 3.1.9 was refocused on providing security notices based on CUI rules. The risk associated with this requirement is low since CUI rules are still in development.
3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.	AC-11	Session Lock	P3	**1**	METHOD(S) TO IMPLEMENT: IT Configuration
		AC-11(1)	Session Lock *Pattern-Hiding Displays*	P3		
3.1.11	Terminate (automatically) a user session after a defined condition.	AC-12	Session Termination	P2	**2**	METHOD(S) TO IMPLEMENT: IT Configuration
3.1.12	Monitor and control remote access sessions.	AC-17(1)	Remote Access *Automated Monitoring / Control*	P1	**5**	METHOD(S) TO IMPLEMENT: Hardware
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	AC-17(2)	Remote Access *Protection of Confidentiality / Integrity Using Encryption*	P1	**5**	METHOD(S) TO IMPLEMENT: Software
3.1.14	Route remote access via managed access control points.	AC-17(3)	Remote Access *Managed Access Control Points*	P1	**5**	METHOD(S) TO IMPLEMENT: Hardware

NIST SP 800-171 Security Requirement		Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171				Table D-2 NIST SP 800-53r4		
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	AC-17(4)	Remote Access *Privileged Commands / Access*	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration
3.1.16	Authorize wireless access prior to allowing such connections.	AC-18	Wireless Access	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration
3.1.17	Protect wireless access using authentication and encryption.	AC-18(1)	Wireless Access *Authentication and Encryption*	P1	**5**	METHOD(S) TO IMPLEMENT: Software
3.1.18	Control connection of mobile devices.	AC-19	Access Control for Mobile Devices	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration
3.1.19	Encrypt CUI on mobile devices and mobile computing platforms.	AC-19(5)	Access Control for Mobile Devices *Full Device / Container-Based Encryption*	P1	**5**	METHOD(S) TO IMPLEMENT: Software
3.1.20	Verify and control/limit connections to and use of external systems.	AC-20	Use of External Systems	P1	**5**	METHOD(S) TO IMPLEMENT: Hardware

NIST SP 800-171 Security Requirement	Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171			Table D-2 NIST SP 800-53r4		
	AC-20(1)	Use of External Systems *Limits on Authorized Use*			
3.1.21 Limit use of organizational portable storage devices on external systems.	AC-20(2)	Use of External Systems *Portable Storage Devices*	P1	**5**	METHOD(S) TO IMPLEMENT: Policy/Process. This requires a policy restricting use of device outside company (e.g., do not use with hotel computers). No IT configuration, or software/hardware required.
3.1.22 Control CUI posted or processed on publicly accessible systems.	AC-22	Publicly Accessible Content	P2	**2**	METHOD(S) TO IMPLEMENT: Policy/Process
3.2 AWARENESS AND TRAINING					
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.	AT-2	Security Awareness Training	P1	**5**	METHOD(S) TO IMPLEMENT: Policy/Process
3.2.2 Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.	AT-3	Role-Based Security Training	P1	**5**	METHOD(S) TO IMPLEMENT: Policy/Process

NIST SP 800-171 Security Requirement	Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171			Table D-2 NIST SP 800-53r4		
3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.	AT-2(2)	Security Awareness Training *Insider Threat*	P1	**2 - 1**	METHOD(S) TO IMPLEMENT: Policy/Process No cost training available at https://www.cdse.edu/catalog/insider-threat.html VALUE: Original NIST SP 800-53 control based on insider risk to classified networks, which does not apply in this case, where assessment of risk is moderate to low.
3.3 AUDIT AND ACCOUNTABILITY					
3.3.1 Create and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.	AU-2	Audit Events	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration
	AU-3	Content of Audit Records	P1		
	AU-3(1)	Content of Audit Records *Additional Audit Information*	P1		
	AU-6	Audit Review, Analysis, and Reporting	P1		
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.	AU-11	Audit Record Retention	P3	**5**	METHOD(S) TO IMPLEMENT: IT Configuration
	AU-12	Audit Generation	P1		

NIST SP 800-171 Security Requirement	Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171			Table D-2 NIST SP 800-53r4		
3.3.3 Review and update audited events.	AU-2(3)	Audit Events *Reviews and Updates*	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration
3.3.4 Alert in the event of an audit process failure.	AU-5	Response to Audit Processing Failures	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration This is typically a standard (default) configuration.
3.3.5 Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	AU-6(3)	Audit Review, Analysis, and Reporting *Correlate Audit Repositories*	P1	**5**	METHOD(S) TO IMPLEMENT: Policy/Process
3.3.6 Provide audit reduction and report generation to support on-demand analysis and reporting.	AU-7	Audit Reduction and Report Generation	P2	**2**	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.	AU-8	Time Stamps	P1	**5/3**	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. VALUE: The lower value may be assigned for small networks not synchronizing with authoritative time source.
	AU-8(1)	Time Stamps *Synchronization with Authoritative Time Source*	P1		

NIST SP 800-171 Security Requirement	Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171			Table D-2 NIST SP 800-53r4		
3.3.8 Protect audit information and audit tools from unauthorized access, modification, and deletion.	AU-9	Protection of Audit Information	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration
3.3.9 Limit management of audit functionality to a subset of privileged users.	AU-9(4)	Protection of Audit Information *Access by Subset of Privileged Users*	P1	**5/3**	METHOD(S) TO IMPLEMENT: IT Configuration VALUE: Businesses with small IT staffs will find it more challenging to separate some privileged duties, but the risk is also less. For small networks the value can be assessed as a 3.
3.4 Configuration Management					
3.4.1 Establish and maintain baseline Configuration and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	CM-2	Baseline Configuration	P1	**5**	METHOD(S) TO IMPLEMENT: Policy/Process or Software
	CM-6	Configuration Settings	P1		
	CM-8	System Component Inventory	P1		
3.4.2 Establish and enforce security configuration settings for information technology products employed in organizational systems.	CM-8(1)	System Component Inventory *Updates During Installations / Removals*	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration or Software

NIST SP 800-171 Security Requirement	Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171			Table D-2 NIST SP 800-53r4		
3.4.3 Track, review, approve or disapprove, and audit changes to organizational systems.	CM-3	Configuration Change Control	P1	**5**	METHOD(S) TO IMPLEMENT: Policy/Process
3.4.4 Analyze the security impact of changes prior to implementation.	CM-4	Security Impact Analysis	P2	**2**	METHOD(S) TO IMPLEMENT: Policy/Process
3.4.5 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	CM-5	Access Restrictions for Change	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration
3.4.6 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	CM-7	Least Functionality	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration
3.4.7 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	CM-7(1)	Least Functionality *Periodic Review*	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration or Software
	CM-7(2)	Least Functionality *Prevent program execution*	P1		METHOD(S) TO IMPLEMENT: IT Configuration or Software

NIST SP 800-171 Security Requirement	Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171			Table D-2 NIST SP 800-53r4		
3.4.8 Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	CM-7(4)	Least Functionality *Unauthorized Software/ Blacklisting*	P1	**5**	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.
	CM-7(5)	Least Functionality *Authorized Software/ Whitelisting*	P1		
3.4.9 Control and monitor user-installed software.	CM-11	User-Installed Software	P1	**5**	METHOD(S) TO IMPLEMENT: Policy/Process, IT Configuration; Software This requirement does not necessarily require use of IT configuration or software. A policy/process of periodic examination of user accounts is acceptable.
3.5 IDENTIFICATION AND AUTHENTICATION					
3.5.1 Identify system users, processes acting on behalf of users, and devices.	IA-2	Identification and Authentication (Organizational Users)	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration
	IA-3	Device Identification and Authentication	P1		
3.5.2 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems.	IA-5	Authenticator Management	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration

NIST SP 800-171 Security Requirement	Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171			Table D-2 NIST SP 800-53r4		
3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	IA-2(1)	Identification and Authentication (Organizational Users) *Network Access to Privileged Accounts*	P1	**5/3**	METHOD(S) TO IMPLEMENT: Hardware/Software VALUE: Lower value should be applied if multifactor authentication has been implemented for privileged and remote users, but not yet implemented for non-remote non-privileged users (i.e., authentication at desktop 'in office').
	IA-2(2)	Identification and Authentication (Organizational Users) *Network Access to Non-Privileged Accounts*	P1		
	IA-2(3)	Identification and Authentication (Organizational Users) *Local Access to Privileged Accounts*	P1		

NIST SP 800-171 Security Requirement		Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171				Table D-2 NIST SP 800-53r4		
3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	IA-2(8)	Identification and Authentication (Organizational Users) *Network Access to Privileged Accounts- Replay Resistant*	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration or Software or Hardware This capability is typically standard on recent Operating Systems.
		IA-2(9)	Identification and Authentication (Organizational Users) *Network Access to Non-Privileged Accounts- Replay Resistant*	P1		
3.5.5	Prevent reuse of identifiers for a defined period.	IA-4	Identifier Management	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration
3.5.6	Disable identifiers after a defined period of inactivity.	IA-4	Identifier Management	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration

NIST SP 800-171 Security Requirement		Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171				Table D-2 NIST SP 800-53r4		
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	IA-5(1)	Authenticator Management *Password-Based Authentication*	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration
3.5.8	Prohibit password reuse for a specified number of generations.				**5**	METHOD(S) TO IMPLEMENT: IT Configuration
3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.				**5**	METHOD(S) TO IMPLEMENT: IT Configuration
3.5.10	Store and transmit only cryptographically-protected passwords.				**5**	METHOD(S) TO IMPLEMENT: IT Configuration
3.5.11	Obscure feedback of authentication information.	IA-6	Authenticator Feedback	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration This is typically a default configuration to replace password text with “dots”.

NIST SP 800-171 Security Requirement		Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171				Table D-2 NIST SP 800-53r4		
3.6						
3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	IR-2	Incident Response Training	P2	**5**	METHOD(S) TO IMPLEMENT: Policy/Process or Software VALUE: While IR Training is assigned a NIST Priority of 2, it does not have a significant effect on value assigned for requirement 3.6.1.
		IR-4	Incident Handling	P1		
3.6.2	Track, document, and report incidents to appropriate organizational officials and/or authorities.	IR-5	Incident Monitoring		**5**	METHOD(S) TO IMPLEMENT: Policy/Process or Software
		IR-6	Incident Reporting	P1		
		IR-7	Incident Response Assistance	P1		
3.6.3	Test the organizational incident response capability.	IR-3	Incident Response Testing	P2	**2**	METHOD(S) TO IMPLEMENT: Policy/Process

NIST SP 800-171 Security Requirement		Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171				Table D-2 NIST SP 800-53r4		
3.7 MAINTENANCE						
3.7.1	Perform maintenance on organizational systems.	MA-2	Controlled Maintenance	P2	**2**	METHOD(S) TO IMPLEMENT: Policy/Process
		MA-3	Maintenance Tools	P2		
3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	MA-3(1)	Maintenance Tools *Inspect Tools*	P2	**2**	METHOD(S) TO IMPLEMENT: Policy/Process
		MA-3(2)	Maintenance Tools *Inspect media*	P2		
3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	MA-2	Controlled Maintenance	P2	**2**	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.	MA-3(2)	Maintenance Tools	P2	**2**	METHOD(S) TO IMPLEMENT: Software
3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	MA-4	Nonlocal Maintenance	P1	**5**	METHOD(S) TO IMPLEMENT: Hardware If remote maintenance sessions are not allowed or company can 'prohibit' remote maintenance access until MFA capability implemented, this requirement is met.

NIST SP 800-171 Security Requirement		Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171				Table D-2 NIST SP 800-53r4		
3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.	MA-5	Maintenance Personnel	P1	**5**	METHOD(S) TO IMPLEMENT: Policy/Process
3.8 MEDIA PROTECTION						
3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	MP-2	Media Access	P1	**5**	METHOD(S) TO IMPLEMENT: Policy/Process
		MP-4	Media Storage	P1		
3.8.2	Limit access to CUI on system media to authorized users.				**5**	METHOD(S) TO IMPLEMENT: Policy/Process
3.8.3	Sanitize or destroy system media containing CUI before disposal or release for reuse.	MP-6	Media Sanitization	P1	**5**	METHOD(S) TO IMPLEMENT: Software
3.8.4	Mark media with necessary CUI markings and distribution limitations.	MP-3	Media Marking	P2	**2**	METHOD(S) TO IMPLEMENT: Policy/Process This requirement applies to the IT system media with CUI (e.g., flash drives, CDs, magnetic tapes, removable hard drives). It is NOT a requirement about marking non-system media (e.g., contract deliverables) with CUI markings.
3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	MP-5	Media Transport	P1	**5**	METHOD(S) TO IMPLEMENT: Policy/Process

NIST SP 800-171 Security Requirement		Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171				Table D-2 NIST SP 800-53r4		
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.	MP-5(4)	Media Transport *Cryptographic Protection*	P1	**5**	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.	MP-7	Media Use	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration A policy and process on allowable use of removable media (e.g., thumb drives, DVDs) would address this requirement.
3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	MP-7(1)	Media Use *Prohibit Use Without Owner*	P1	**5**	METHOD(S) TO IMPLEMENT: Policy/Process A policy prohibiting use of anonymous portable storage devices (e.g., thumb drives) and a process to check on compliance would address this requirement.
3.8.9	Protect the confidentiality of backup CUI at storage locations.	CP-9	System Backup	P1	**5**	METHOD(S) TO IMPLEMENT: Policy/Process or Software

NIST SP 800-171 Security Requirement	Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171			Table D-2 NIST SP 800-53r4		
3.9 PERSONNEL SECURITY					
3.9.1 Screen individuals prior to authorizing access to organizational systems containing CUI.	PS-3	Personnel Screening	P1	**5**	METHOD(S) TO IMPLEMENT: Policy/Process
	PS-4	Personnel Termination	P1		
3.9.2 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	PS-5	Personnel Transfer	P2	**5/3**	METHOD(S) TO IMPLEMENT: Policy/Process VALUE: A lower value of 3 should be assigned if implemented for personnel termination but not yet for personnel transfer.
3.10 PHYSICAL PROTECTION					
3.10.1 Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	PE-2	Physical Access Authorizations	P1	**5/3**	METHOD(S) TO IMPLEMENT: Policy/Process, Software, Hardware Businesses with IT systems that are not in restricted spaces (e.g., distributed within office environment) may meet this require through observation/escort procedures. VALUE: Lower value of 3 may be assigned if access to output devices (e.g., printers) is not limited.
	PE-4	Access Control for Transmission Medium	P1		
	PE-5	Access Control for Output Devices	P2		
3.10.2 Protect and monitor the physical facility and support infrastructure for those systems.	PE-6	Monitoring Physical Access	P1	**5**	METHOD(S) TO IMPLEMENT: Policy/Process, Software, Hardware
3.10.3 Escort visitors and monitor visitor activity.	PE-3	Physical Access Control	P1	**5**	METHOD(S) TO IMPLEMENT: Policy/Process

NIST SP 800-171 Security Requirement	Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171			Table D-2 NIST SP 800-53r4		
3.10.4 Maintain audit logs of physical access.			P1	**5**	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.			P1	**5**	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.	PE-17	Alternate Work Site	P2	**2**	METHOD(S) TO IMPLEMENT: Policy/Process
3.11 RISK ASSESSMENT					
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.	RA-3	Risk Assessment	P1	**5**	METHOD(S) TO IMPLEMENT: Policy/Process
3.11.2 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	RA-5	Vulnerability Scanning	P1	**5**	METHOD(S) TO IMPLEMENT: Software
	RA-5(5)	Vulnerability Scanning *Privileged Access*	P1		

NIST SP 800-171 Security Requirement	Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171			Table D-2 NIST SP 800-53r4		
3.11.3 Remediate vulnerabilities in accordance with assessments of risk.	RA-5	Vulnerability Scanning	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration
3.12 SECURITY ASSESMENT					
3.12.1 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application	CA-2	Security Assessments	P2	**2**	METHOD(S) TO IMPLEMENT: Policy/Process
3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	CA-5	Plan of Action and Milestones	P3	**5**	METHOD(S) TO IMPLEMENT: Policy/Process 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 deficiencies have been identified, no plan of action is required. VALUE: While listed as a Priority 3, 3.12.2 is required to demonstrate compliance with NIST SP 800-171.
3.12.3 Monitor security controls on ongoing basis to ensure continued effectiveness of controls.	CA-7	Continuous Monitoring	P3	**1**	METHOD(S) TO IMPLEMENT: Policy/Process or Software
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.	PL-2	System Security Plan	P1	**5**	METHOD(S) TO IMPLEMENT: Policy/Process

NIST SP 800-171 Security Requirement	Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171			Table D-2 NIST SP 800-53r4		
3.13 SYSTEM AND COMMUNICATIONS PROTECTION					
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.	SC-7	Boundary Protection	P1	**5**	METHOD(S) TO IMPLEMENT: Hardware
3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	SA-8	Security Engineering Principles	P1	**5/1**	METHOD(S) TO IMPLEMENT: Policy/Process VALUE: For businesses using standard COTS products and network designs risk will be lower as the software or system engineering designs already exist. If this is the case, risk be assessed as low (1).
3.13.3 Separate user functionality from system management functionality.	SC-2	Application Partitioning	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration
3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.	SC-4	Information in Shared Resources	P1	**5**	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.	SC-7	Boundary Protection	P1	**5**	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	Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171			Table D-2 NIST SP 800-53r4		
3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	SC-7(5)	Boundary Protection *Deny by Default / Allow by Exception*	P1	**5**	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.
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).	SC-7(7)	Boundary Protection *Prevent Split Tunneling for Remote Devices*	P1	**5**	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.	SC-8	Transmission Confidentiality and Integrity	P1	5	METHOD(S) TO IMPLEMENT: IT Configuration or Software or Hardware
	SC-8(1)	Transmission Confidentiality and Integrity *Cryptographic or Alternate Physical Protection*			
3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	SC-10	Network Disconnect	P2	2	METHOD(S) TO IMPLEMENT: IT Configuration

NIST SP 800-171 Security Requirement	Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171			Table D-2 NIST SP 800-53r4		
3.13.10 Establish and manage cryptographic keys for cryptography employed in organizational systems.	SC-12	Cryptographic Key Establishment and Management	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration or Software
3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	SC-13	Cryptographic Protection	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration or Software or Hardware 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.	SC-15	Collaborative Computing Devices	P1	**5**	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.	SC-18	Mobile Code	P2	**2**	METHOD(S) TO IMPLEMENT: IT Configuration or Software or Hardware
3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	SC-19	Voice over Internet Protocol	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration or Software or Hardware This requires treating VoIP as IP (e.g., configuring firewalls appropriately). It does NOT require monitoring content of calls.
3.13.15 Protect the authenticity of communications sessions.	SC-23	Session Authenticity	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration This is often a default configuration.

NIST SP 800-171 Security Requirement	Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171			Table D-2 NIST SP 800-53r4		
3.13.16 Protect the confidentiality of CUI at rest.	SC-28	Protection of Information at Rest	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration or Software 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).
3.14 SYSTEM AND INFORMATION INTEGRITY					
3.14.1 Identify, report, and correct system flaws in a timely manner.	SI-2	Flaw Remediation	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration or Software
3.14.2 Provide protection from malicious code at appropriate locations within organizational systems.	SI-3	Malicious Code Protection	P1	**5**	METHOD(S) TO IMPLEMENT: Software
3.14.3 Monitor system security alerts and advisories and take action in response.	SI-5	Security Alerts, Advisories, and Directives	P1	**5**	METHOD(S) TO IMPLEMENT: Policy or Software
3.14.4 Update malicious code protection mechanisms when new releases are available.	SI-3	Malicious Code Protection	P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration
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.			P1	**5**	METHOD(S) TO IMPLEMENT: IT Configuration

NIST SP 800-171 Security Requirement	Corresponding NIST SP 800-53 Security Controls		NIST Priority	DoD Value High (5-3) Mod (2) Low (1)	Comments
Table D-14 NIST SP 800-171			Table D-2 NIST SP 800-53r4		
3.14.6 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	SI-4	System Monitoring	P1	**5**	METHOD(S) TO IMPLEMENT: Software or Hardware
	SI-4(4)	System Monitoring *Inbound and Outbound Communications Traffic*			
3.14.7 Identify unauthorized use of organizational systems.	SI-4	System Monitoring	P1	**5**	METHOD(S) TO IMPLEMENT: Software or Hardware