ATTACHMENT J-3
Security Controls for Information Systems
Definitions from NIST Special Publication 800-53

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
FIPS Pub 200 Definition for High/Moderate/Low Impact Information System:			FIPS Publication 199 requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. Since the potential impact values for confidentiality, integrity, and availability may not always be the same for a particular information system, the high water mark concept must be used to determine the overall impact level of the information system. Thus, a **low-impact system** is an information system in which all three of the security objectives are low. A **moderate-impact system** is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate. And finally, a **high-impact system** is an information system in which at least one security objective is high. The determination of information system impact levels must be accomplished prior to the consideration of minimum security requirements and the selection of appropriate security controls for those information systems.		
DoDI 8500.2 Mission Assurance Category (MAC) Definitions:			Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. Mission Assurance Category I systems require the most stringent protection measures.	Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. Mission Assurance Category II systems require additional safeguards beyond best practices to ensure assurance.	Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. **Mission Assurance Category III systems require protective measures, techniques, or procedures generally**

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
					commensurate with commercial best practices.
Access Control					
ECAN-1 ECPA-1 PRAS-1 DCAR-1	AC-1	ACCESS CONTROL POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.
IAAC-1	AC-2	ACCOUNT MANAGEMENT	The organization manages information system accounts, including: a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary); b. Establishing conditions for group membership; c. Identifying authorized users of the information system and specifying access privileges; d. Requiring appropriate approvals for requests to establish accounts; e. Establishing, activating, modifying, disabling, and removing accounts; f. Specifically authorizing and	The organization manages information system accounts, including: a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary); b. Establishing conditions for group membership; c. Identifying authorized users of the information system and specifying access privileges; d. Requiring appropriate approvals for requests to establish accounts; e. Establishing, activating, modifying, disabling, and removing accounts;	The organization manages information system accounts, including: a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary); b. Establishing conditions for group membership; c. Identifying authorized users of the information system and specifying access privileges; d. Requiring appropriate approvals for requests to establish accounts; e. Establishing, activating,

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			monitoring the use of guest/anonymous and temporary accounts; g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes; h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users; i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and j. Reviewing accounts [*Assignment: organization-defined frequency*]. Control Enhancements: (1) The organization employs automated mechanisms to support the management of information system accounts. (2) The information system automatically terminates temporary and emergency accounts after [*Assignment: organization-defined time period for each type of account*]. (3) The information system	f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes; h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users; i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and j. Reviewing accounts [*Assignment: organization-defined frequency*]. Control Enhancements: (1) The organization employs automated mechanisms to support the management of information system accounts. (2) The information system automatically terminates temporary	modifying, disabling, and removing accounts; f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes; h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users; i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and j. Reviewing accounts [*Assignment: organization-defined frequency*].

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			automatically disables inactive accounts after [*Assignment: organization-defined time period*]. (4) The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.	and emergency accounts after [*Assignment: organization-defined time period for each type of account*]. (3) The information system automatically disables inactive accounts after [*Assignment: organization-defined time period*]. (4) The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.	
DCFA-1 ECAN-1 EBRU-1 PRNK-1 ECCD-1 ECSD-2	AC-3	ACCESS ENFORCEMENT	The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.	The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.	The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.
EBBD-1 EBBD-2	AC-4	INFORMATION FLOW ENFORCEMENT	The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy	The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	Not Applicable
ECLP-1	AC-5	SEPARATION OF DUTIES	The organization: a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion;	The organization: a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion;	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			b. Documents separation of duties; and c. Implements separation of duties through assigned information system access authorizations.	b. Documents separation of duties; and c. Implements separation of duties through assigned information system access authorizations.	
ECLP-1	AC-6	LEAST PRIVILEGE	The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. Control Enhancements: (1) The organization explicitly authorizes access to [*Assignment: organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information*]. (2) The organization requires that users of information system accounts, or roles, with access to [*Assignment: organization-defined list of security functions or security-relevant information*], use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.	The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. Control Enhancements: (1) The organization explicitly authorizes access to [*Assignment: organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information*]. (2) The organization requires that users of information system accounts, or roles, with access to [*Assignment: organization-defined list of security functions or security-relevant information*], use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.	Not Applicable

References			Task Order Requirement		
DoDI 8500.2	**NIST 800-53**	**CONTROL NAME**	**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
ECLO-1	AC-7	UNSUCCESSFUL LOGIN ATTEMPTS	The information system: a. Enforces a limit of [*Assignment: organization-defined number*] consecutive invalid access attempts by a user during a [*Assignment: organization-defined time period*]; and b. Automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*]; *locks the account/node until released by an administrator; delays next login prompt according to* [*Assignment: organization-defined delay algorithm*]] when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.	The information system: a. Enforces a limit of [*Assignment: organization-defined number*] consecutive invalid access attempts by a user during a [*Assignment: organization-defined time period*]; and b. Automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*]; *locks the account/node until released by an administrator; delays next login prompt according to* [*Assignment: organization-defined delay algorithm*]] when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.	The information system: a. Enforces a limit of [*Assignment: organization-defined number*] consecutive invalid access attempts by a user during a [*Assignment: organization-defined time period*]; and b. Automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*]; *locks the account/node until released by an administrator; delays next login prompt according to* [*Assignment: organization-defined delay algorithm*]] when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.
ECWM-1	AC-8	SYSTEM USE NOTIFICATION	The information system: a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is	The information system: a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use	The information system: a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded,

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.	of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.	and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.
	AC-9	PREVIOUS LOGON (ACCESS) NOTIFICATION	Not Applicable	Not Applicable	Not Applicable
ECLO-1	AC-10	CONCURRENT SESSION CONTROL	The information system limits the number of concurrent sessions for each system account to [*Assignment: organization-defined number*].	Not Applicable	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
PESL-1	AC-11	SESSION LOCK	The information system: a. Prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.	The information system: a. Prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.	Not Applicable
---	AC-12	SESSION TERMINATION	Withdrawn: Incorporated into SC-10.	Withdrawn: Incorporated into SC-10.	Withdrawn: Incorporated into SC-10
ECAT-1 ECAT-2 E3.3.9	AC-13	SUPERVISION AND REVIEW — ACCESS CONTROL	Withdrawn: Incorporated into AC-2 and AU-6.	Withdrawn: Incorporated into AC-2 and AU-6.	Withdrawn: Incorporated into AC-2 and AU-6.
---	AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	The organization: a. Identifies specific user actions that can be performed on the information system without identification or authentication; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication. Control Enhancement: (1) The organization permits actions to be performed without identification and	The organization: a. Identifies specific user actions that can be performed on the information system without identification or authentication; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication. Control Enhancement: (1) The organization permits actions to be performed without identification	The organization: a. Identifies specific user actions that can be performed on the information system without identification or authentication; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			authentication only to the extent necessary to accomplish mission/business objectives.	and authentication only to the extent necessary to accomplish mission/business objectives.	
ECML-1	AC-15	AUTOMATED MARKING	Withdrawn: Incorporated into MP-3.	Withdrawn: Incorporated into MP-3.	Withdrawn: Incorporated into MP-3.
	AC-16	SECURITY ATTRIBUTES	Not Applicable	Not Applicable	Not Applicable
EBRP-1 EBRU-1	AC-17	REMOTE ACCESS	The organization: a. Documents allowed methods of remote access to the information system; b. Establishes usage restrictions and implementation guidance for each allowed remote access method; c. Monitors for unauthorized remote access to the information system; d. Authorizes remote access to the information system prior to connection; and e. Enforces requirements for remote connections to the information system. Control Enhancements: (1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods. (2) The organization uses cryptography to protect the confidentiality and	The organization: a. Documents allowed methods of remote access to the information system; b. Establishes usage restrictions and implementation guidance for each allowed remote access method; c. Monitors for unauthorized remote access to the information system; d. Authorizes remote access to the information system prior to connection; and e. Enforces requirements for remote connections to the information system. Control Enhancements: (1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods. (2) The organization uses	The organization: a. Documents allowed methods of remote access to the information system; b. Establishes usage restrictions and implementation guidance for each allowed remote access method; c. Monitors for unauthorized remote access to the information system; d. Authorizes remote access to the information system prior to connection; and e. Enforces requirements for remote connections to the information system.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			integrity of remote access sessions. (3) The information system routes all remote accesses through a limited number of managed access control points. (4) The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system. (5) The organization monitors for unauthorized remote connections to the information system [*Assignment: organization-defined frequency*], and takes appropriate action if an unauthorized connection is discovered. (7) The organization ensures that remote sessions for accessing [*Assignment: organization-defined list of security functions and security-relevant information*] employ [*Assignment: organization-defined additional security measures*] and are audited. (8) The organization disables networking protocols within the information system deemed to be nonsecure except for explicitly identified components in support of specific operational requirements.	cryptography to protect the confidentiality and integrity of remote access sessions. (3) The information system routes all remote accesses through a limited number of managed access control points. (4) The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system. (5) The organization monitors for unauthorized remote connections to the information system [*Assignment: organization-defined frequency*], and takes appropriate action if an unauthorized connection is discovered. (7) The organization ensures that remote sessions for accessing [*Assignment: organization-defined list of security functions and security-relevant information*] employ [*Assignment: organization-defined additional security measures*] and are audited. (8) The organization disables networking protocols within the information system deemed to be	

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
				nonsecure except for explicitly identified components in support of specific operational requirements.	
ECCT-1 ECWN-1	AC-18	WIRELESS ACCESS	The organization: a. Establishes usage restrictions and implementation guidance for wireless access; b. Monitors for unauthorized wireless access to the information system; c. Authorizes wireless access to the information system prior to connection; and d. Enforces requirements for wireless connections to the information system. Control Enhancements: (1) The information system protects wireless access to the system using authentication and encryption. (2) The organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points [*Assignment: organization-defined frequency*], and takes appropriate action if an unauthorized connection is discovered. (4) The organization does not allow users to independently configure wireless networking capabilities. (5) The organization confines wireless	The organization: a. Establishes usage restrictions and implementation guidance for wireless access; b. Monitors for unauthorized wireless access to the information system; c. Authorizes wireless access to the information system prior to connection; and d. Enforces requirements for wireless connections to the information system. Control Enhancement: (1) The information system protects wireless access to the system using authentication and encryption.	The organization: a. Establishes usage restrictions and implementation guidance for wireless access; b. Monitors for unauthorized wireless access to the information system; c. Authorizes wireless access to the information system prior to connection; and d. Enforces requirements for wireless connections to the information system.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			communications to organization-controlled boundaries.		
ECWN-1	AC-19	ACCESS CONTROL FOR MOBILE DEVICES	The organization: a. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices; b. Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems; c. Monitors for unauthorized connections of mobile devices to organizational information systems; d. Enforces requirements for the connection of mobile devices to organizational information systems; e. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction; f. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and g. Applies [*Assignment: organization-defined inspection and preventative measures*] to mobile devices returning from locations that the organization deems to be of significant risk in	The organization: a. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices; b. Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems; c. Monitors for unauthorized connections of mobile devices to organizational information systems; d. Enforces requirements for the connection of mobile devices to organizational information systems; e. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction; f. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and g. Applies [*Assignment: organization-defined inspection and preventative measures*] to mobile devices returning	The organization: a. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices; b. Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems; c. Monitors for unauthorized connections of mobile devices to organizational information systems; d. Enforces requirements for the connection of mobile devices to organizational information systems; e. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction; f. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and g. Applies [*Assignment: organization-defined inspection and preventative measures*] to mobile

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			accordance with organizational policies and procedures. Control Enhancements: (1) The organization restricts the use of writable, removable media in organizational information systems. (2) The organization prohibits the use of personally owned, removable media in organizational information systems. (3) The organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner.	from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures. Control Enhancements: (1) The organization restricts the use of writable, removable media in organizational information systems. (2) The organization prohibits the use of personally owned, removable media in organizational information systems. (3) The organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner.	devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.
---	AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from the external information systems; and b. Process, store, and/or transmit organization-controlled information using the external information systems. Control Enhancements:	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from the external information systems; and b. Process, store, and/or transmit organization-controlled information using the external information systems.	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from the external information systems; and b. Process, store, and/or transmit organization-controlled information using the external information systems.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			(1) The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: (a) Can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or (b) Has approved information system connection or processing agreements with the organizational entity hosting the external information system. (2) The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.	Control Enhancements: (1) The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: (a) Can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or (b) Has approved information system connection or processing agreements with the organizational entity hosting the external information system. (2) The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.	
	AC-21	USER-BASED COLLABORATION AND INFORMATION SHARING	Not Applicable	Not Applicable	Not Applicable
	AC-22	PUBLICLY ACCESSIBLE CONTENT	The organization: a. Designates individuals authorized to post information onto an organizational information system that is publicly	The organization: a. Designates individuals authorized to post information onto an organizational information system that	The organization: a. Designates individuals authorized to post information onto an organizational information system

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			accessible; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system; d. Reviews the content on the publicly accessible organizational information system for nonpublic information [*Assignment: organization-defined frequency*]; and e. Removes nonpublic information from the publicly accessible organizational information system, if discovered.	is publicly accessible; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system; d. Reviews the content on the publicly accessible organizational information system for nonpublic information [*Assignment: organization-defined frequency*]; and e. Removes nonpublic information from the publicly accessible organizational information system, if discovered.	that is publicly accessible; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system; d. Reviews the content on the publicly accessible organizational information system for nonpublic information [*Assignment: organization-defined frequency*]; and e. Removes nonpublic information from the publicly accessible organizational information system, if discovered.
Awareness and Training					
PRTN-1 DCAR-1	AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.
PRTN-1	AT-2	SECURITY AWARENESS	The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and [*Assignment: organization-defined frequency*] thereafter.	The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and [*Assignment: organization-defined frequency*] thereafter.	The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and [*Assignment: organization-defined frequency*] thereafter.
PRTN-1	AT-3	SECURITY TRAINING	The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment: organization-defined frequency*] thereafter.	The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment: organization-defined frequency*] thereafter.	The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment: organization-defined frequency*] thereafter.
---	AT-4	SECURITY TRAINING RECORDS	The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for [*Assignment: organization-defined time period*].	The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for [*Assignment: organization-defined time period*].	The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for [*Assignment: organization-defined time period*].

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
	AT-5	CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS	Not Applicable	Not Applicable	Not Applicable
Audit and Accountability					
ECAT-1 ECTB-1 DCAR-1	AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.
ECAR-3	AU-2	AUDITABLE EVENTS	The organization: a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: [*Assignment: organization-defined list of auditable events*]; b. Coordinates the security audit function with other organizational entities requiring audit-related	The organization: a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: [*Assignment: organization-defined list of auditable events*]; b. Coordinates the security audit function with other organizational	The organization: a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: [*Assignment: organization-defined list of auditable events*]; b. Coordinates the security audit function with other organizational

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [*Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited along with the frequency of (or situation requiring) auditing for each identified event*]. Control Enhancements: (3) The organization reviews and updates the list of auditable events [*Assignment: organization-defined frequency*]. (4) The organization includes execution of privileged functions in the list of events to be audited by the information system.	entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [*Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited along with the frequency of (or situation requiring) auditing for each identified event*]. Control Enhancements: (3) The organization reviews and updates the list of auditable events [*Assignment: organization-defined frequency*]. (4) The organization includes execution of privileged functions in the list of events to be audited by the information system.	entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [*Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited along with the frequency of (or situation requiring) auditing for each identified event*].
ECAR-1 ECAR-2	AU-3	CONTENT OF AUDIT RECORDS	The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date	The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred,	The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
ECAR-3 ECLC-1			and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event. Control Enhancements: (1) The information system includes [*Assignment: organization-defined additional, more detailed information*] in the audit records for audit events identified by type, location, or subject. (2) The organization centrally manages the content of audit records generated by [*Assignment: organization-defined information system components*].	when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event. Control Enhancement: (1) The information system includes [*Assignment: organization-defined additional, more detailed information*] in the audit records for audit events identified by type, location, or subject.	occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.
---	AU-4	AUDIT STORAGE CAPACITY	The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.
---	AU-5	RESPONSE TO AUDIT PROCESSING FAILURES	The information system: a. Alerts designated organizational officials in the event of an audit processing failure; and b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].	The information system: a. Alerts designated organizational officials in the event of an audit processing failure; and b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].	The information system: a. Alerts designated organizational officials in the event of an audit processing failure; and b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			Control Enhancements: (1) The information system provides a warning when allocated audit record storage volume reaches [*Assignme*nt: organi*zation-defined percentage*] of maximum audit record storage capacity. (2) The information system provides a real-time alert when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].		
ECAT-1 E3.3.9	AU-6	AUDIT REVIEW, ANALYSIS, AND REPORTING	The organization: a. Reviews and analyzes information system audit records [*Assignment: organization-defined frequency*] for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information. Control Enhancement: (1) The information system integrates	The organization: a. Reviews and analyzes information system audit records [*Assignment: organization-defined frequency*] for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.	The organization: a. Reviews and analyzes information system audit records [*Assignment: organization-defined frequency*] for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.		
ECRG-1	AU-7	AUDIT REDUCTION AND REPORT GENERATION	The information system provides an audit reduction and report generation capability. Control Enhancement: (1) The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.	The information system provides an audit reduction and report generation capability. Control Enhancement: (1) The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.	Not Applicable
ECAR-1	AU-8	TIME STAMPS	The information system uses internal system clocks to generate time stamps for audit records. Control Enhancement: (1) The information system synchronizes internal information system clocks [*Assignment: organization-defined frequency*] with [*Assignment: organization-defined authoritative time source*].	The information system uses internal system clocks to generate time stamps for audit records. Control Enhancement: (1) The information system synchronizes internal information system clocks [*Assignment: organization-defined frequency*] with [*Assignment: organization-defined authoritative time source*].	The information system uses internal system clocks to generate time stamps for audit records.
ECTP-1	AU-9	PROTECTION OF AUDIT INFORMATION	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.
	AU-10	NON-REPUDIATION	The information system protects against an individual falsely denying having performed a particular action.	Not Applicable	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
ECRR-1	AU-11	AUDIT RECORD RETENTION	The organization retains audit records for [*Assignment: organization-defined time period consistent with records retention policy*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	The organization retains audit records for [*Assignment: organization-defined time period consistent with records retention policy*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	The organization retains audit records for [*Assignment: organization-defined time period consistent with records retention policy*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
	AU-12	AUDIT GENERATION	The information system: a. Provides audit record generation capability for the list of auditable events defined in AU-2 at [*Assignment: organization-defined information system components*]; b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3. Control Enhancement: (1) The information system compiles audit records from [*Assignment: organization-defined information system components*] into a system-wide (logical or physical) audit trail that is time-correlated to within [*Assignment: organization-defined level of tolerance for relationship between time stamps of*	The information system: a. Provides audit record generation capability for the list of auditable events defined in AU-2 at [*Assignment: organization-defined information system components*]; b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.	The information system: a. Provides audit record generation capability for the list of auditable events defined in AU-2 at [*Assignment: organization-defined information system components*]; b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			individual records in the audit trail].		
	AU-13	MONITORING FOR INFORMATION DISCLOSURE	Not Applicable	Not Applicable	Not Applicable
	AU-14	SESSION AUDIT	Not Applicable	Not Applicable	Not Applicable
Security Assessment and Authorization					
DCAR-1 DCII-1	CA-1	SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.
DCII-1 ECMT-1 PEPS-1 E3.3.10	CA-2	SECURITY ASSESSMENTS	The organization: a. Develops a security assessment plan that describes the scope of the assessment including: - Security controls and control enhancements under assessment; - Assessment procedures to be used to	The organization: a. Develops a security assessment plan that describes the scope of the assessment including: - Security controls and control enhancements under assessment; - Assessment procedures to be used	The organization: a. Develops a security assessment plan that describes the scope of the assessment including: - Security controls and control enhancements under assessment; - Assessment procedures to be

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			determine security control effectiveness; and - Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative. Control Enhancements: (1) The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system. (2) The organization includes as part of security control assessments, [*Assignment: organization-defined frequency*], [*Selection: announced;*	to determine security control effectiveness; and - Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative. Control Enhancement: (1) The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.	used to determine security control effectiveness; and - Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative. .

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			unannounced], [*Selection: in-depth monitoring; malicious user testing; penetration testing; red team exercises;* [*Assignment: organization-defined other forms of security testing*]].		
DCID-1 EBCR-1 EBRU-1 EBPW-1 ECIC-1	CA-3	INFORMATION SYSTEM CONNECTIONS	The organization: a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements; b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.	The organization: a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements; b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.	The organization: a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements; b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.
DCAR-1 5.7.5	CA-4	SECURITY CERTIFICATION	Withdrawn: Incorporated into CA-2.	Withdrawn: Incorporated into CA-2.	Withdrawn: Incorporated into CA-2.
5.7.5	CA-5	PLAN OF ACTION AND MILESTONES	The organization: a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known	The organization: a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate	The organization: a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			vulnerabilities in the system; and b. Updates existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	known vulnerabilities in the system; and b. Updates existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	and to reduce or eliminate known vulnerabilities in the system; and b. Updates existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.
5.7.5	CA-6	SECURITY AUTHORIZATION	The organization: a. Assigns a senior-level executive or manager to the role of authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization [*Assignment: organization-defined frequency*].	The organization: a. Assigns a senior-level executive or manager to the role of authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization [*Assignment: organization-defined frequency*].	The organization: a. Assigns a senior-level executive or manager to the role of authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization [*Assignment: organization-defined frequency*].
DCCB-1 DCPR-1 E3.3.9	CA-7	CONTINUOUS MONITORING	The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: a. A configuration management process for the information system and its constituent components; b. A determination of the security impact of changes to the information system and environment of operation; c. Ongoing security control assessments in accordance with the	The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: a. A configuration management process for the information system and its constituent components; b. A determination of the security impact of changes to the information system and environment of operation; c. Ongoing security control assessments in accordance with the	The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: a. A configuration management process for the information system and its constituent components; b. A determination of the security impact of changes to the information system and environment of operation; c. Ongoing security control

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			organizational continuous monitoring strategy; and d. Reporting the security state of the information system to appropriate organizational officials [*Assignment: organization-defined frequency*].	organizational continuous monitoring strategy; and d. Reporting the security state of the information system to appropriate organizational officials [*Assignment: organization-defined frequency*].	assessments in accordance with the organizational continuous monitoring strategy; and d. Reporting the security state of the information system to appropriate organizational officials [*Assignment: organization-defined frequency*].
Configuration Management					
DCCB-1 DCPR-1 DCAR-1 E3.3.8	CM-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.
DCHW-1 DCSW-1	CM-2	BASELINE CONFIGURATION	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system. Control Enhancements: (1) The organization reviews and updates the baseline configuration of	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system. Control Enhancements: (1) The organization reviews and	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			the information system: (a) [*Assignment: organization-defined frequency*]; (b) When required due to [*Assignment organization-defined circumstances*]; and (c) As an integral part of information system component installations and upgrades. (2) The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system. (3) The organization retains older versions of baseline configurations as deemed necessary to support rollback. (5) The organization: (a) Develops and maintains [*Assignment: organization-defined list of software programs authorized to execute on the information system*]; and (b) Employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system. (6) The organization maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.	updates the baseline configuration of the information system: (a) [*Assignment: organization-defined frequency*]; (b) When required due to [*Assignment organization-defined circumstances*]; and (c) As an integral part of information system component installations and upgrades. (3) The organization retains older versions of baseline configurations as deemed necessary to support rollback. (4) The organization: (a) Develops and maintains [*Assignment: organization-defined list of software programs not authorized to execute on the information system*]; and (b) Employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system.	
DCPR-1	CM-3	CONFIGURATION CHANGE	The organization: a. Determines the types of changes to	The organization: a. Determines the types of changes to	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
		CONTROL	the information system that are configuration controlled; b. Approves configuration-controlled changes to the system with explicit consideration for security impact analyses; c. Documents approved configuration-controlled changes to the system; d. Retains and reviews records of configuration-controlled changes to the system; e. Audits activities associated with configuration-controlled changes to the system; and f. Coordinates and provides oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element (e.g., committee, board*] that convenes [*Selection: (one or more):* [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined configuration change conditions*]]. Control Enhancements: (1) The organization employs automated mechanisms to: (a) Document proposed changes to the information system; (b) Notify designated approval authorities;	the information system that are configuration controlled; b. Approves configuration-controlled changes to the system with explicit consideration for security impact analyses; c. Documents approved configuration-controlled changes to the system; d. Retains and reviews records of configuration-controlled changes to the system; e. Audits activities associated with configuration-controlled changes to the system; and f. Coordinates and provides oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element (e.g., committee, board*] that convenes [*Selection: (one or more):* [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined configuration change conditions*]]. Control Enhancement: (2) The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.	

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			(c) Highlight approvals that have not been received; (d) Inhibit change until designated approvals are received; and (e) Document completed changes to the information system. (2) The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.		
DCPR-1 E3.3.8	CM-4	SECURITY IMPACT ANALYSIS	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation. Control Enhancement: (1) The organization analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.
DCPR-1 ECSD-2	CM-5	ACCESS RESTRICTIONS FOR CHANGE	The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. Control Enhancements: (1) The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions. (2) The organization conducts audits of	The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			information system changes [*Assignment: organization-defined frequency*] and when indications so warrant to determine whether unauthorized changes have occurred. (3) The information system prevents the installation of [*Assignment: organization-defined critical software programs*] that are not signed with a certificate that is recognized and approved by the organization.		
DCSS-1 ECSC-1 E3.3.8	CM-6	CONFIGURATION SETTINGS	The organization: a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	The organization: a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	The organization: a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			Control Enhancements: (1) The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings. (2) The organization employs automated mechanisms to respond to unauthorized changes to [*Assignment: organization-defined configuration settings*]. (3) The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.	Control Enhancement: (3) The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.	
DCPP-1 ECIM-1 ECVI-1 E3.3.8	CM-7	LEAST FUNCTIONALITY	The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services*]. Control Enhancements: (1) The organization reviews the information system [*Assignment:*	The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services*]. Control Enhancement: (1) The organization reviews the information system [*Assignment:*	The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services*].

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			organization-defined frequency] to identify and eliminate unnecessary functions, ports, protocols, and/or services. (2) The organization employs automated mechanisms to prevent program execution in accordance with [*Selection (one or more): list of authorized software programs; list of unauthorized software programs; rules authorizing the terms and conditions of software program usage*].	*organization-defined frequency*] to identify and eliminate unnecessary functions, ports, protocols, and/or services.	
	CM-8	INFORMATION SYSTEM COMPONENT INVENTORY	The organization develops, documents, and maintains an inventory of information system components that: a. Accurately reflects the current information system; b. Is consistent with the authorization boundary of the information system; c. Is at the level of granularity deemed necessary for tracking and reporting; d. Includes [*Assignment: organization-defined information deemed necessary to achieve effective property accountability*]; and e. Is available for review and audit by designated organizational officials. Control Enhancements: (1) The organization updates the inventory of information system components as an integral part of	The organization develops, documents, and maintains an inventory of information system components that: a. Accurately reflects the current information system; b. Is consistent with the authorization boundary of the information system; c. Is at the level of granularity deemed necessary for tracking and reporting; d. Includes [*Assignment: organization-defined information deemed necessary to achieve effective property accountability*]; and e. Is available for review and audit by designated organizational officials. Control Enhancements: (1) The organization updates the inventory of information system	The organization develops, documents, and maintains an inventory of information system components that: a. Accurately reflects the current information system; b. Is consistent with the authorization boundary of the information system; c. Is at the level of granularity deemed necessary for tracking and reporting; d. Includes [*Assignment: organization-defined information deemed necessary to achieve effective property accountability*]; and e. Is available for review and audit by designated organizational officials.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			component installations, removals, and information system updates. (2) The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components. (3) The organization: (a) Employs automated mechanisms [*Assignment: organization-defined frequency*] to detect the addition of unauthorized components/devices into the information system; and (b) Disables network access by such components/devices or notifies designated organizational officials. (4) The organization includes in property accountability information for information system components, a means for identifying by [*Selection (one or more): name; position; role*] individuals responsible for administering those components. (5) The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.	components as an integral part of component installations, removals, and information system updates. (5) The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.	
	CM-9	CONFIGURATION MANAGEMENT	The organization develops, documents, and implements a configuration	The organization develops, documents, and implements a	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
		PLAN	management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.	configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.	
Contingency Planning					
COBR-1 DCAR-1	CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
				controls.	controls.
CODP-1 COEF-1	CP-2	CONTINGENCY PLAN	The organization: a. Develops a contingency plan for the information system that: - Identifies essential missions and business functions and associated contingency requirements; - Provides recovery objectives, restoration priorities, and metrics; - Addresses contingency roles, responsibilities, assigned individuals with contact information; - Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; - Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the contingency plan to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the	The organization: a. Develops a contingency plan for the information system that: - Identifies essential missions and business functions and associated contingency requirements; - Provides recovery objectives, restoration priorities, and metrics; - Addresses contingency roles, responsibilities, assigned individuals with contact information; - Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; - Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the contingency plan to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*]; c. Coordinates contingency planning activities with incident handling	The organization: a. Develops a contingency plan for the information system that: - Identifies essential missions and business functions and associated contingency requirements; - Provides recovery objectives, restoration priorities, and metrics; - Addresses contingency roles, responsibilities, assigned individuals with contact information; - Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; - Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the contingency plan to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*]; c. Coordinates contingency planning activities with incident handling

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			information system [*Assignment: organization-defined frequency*]; e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and f. Communicates contingency plan changes to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*]. Control Enhancements: (1) The organization coordinates contingency plan development with organizational elements responsible for related plans. (2) The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations. (3) The organization plans for the resumption of essential missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation.	activities; d. Reviews the contingency plan for the information system [*Assignment: organization-defined frequency*]; e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and f. Communicates contingency plan changes to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*]. Control Enhancement: (1) The organization coordinates contingency plan development with organizational elements responsible for related plans.	activities; d. Reviews the contingency plan for the information system [*Assignment: organization-defined frequency*]; e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and f. Communicates contingency plan changes to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*].

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
PRTN-1	CP-3	CONTINGENCY TRAINING	The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency*]. Control Enhancements: (1) The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.	The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency*].	The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency*].
COED-1	CP-4	CONTINGENCY PLAN TESTING AND EXERCISES	The organization: a. Tests and/or exercises the contingency plan for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests and/or exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan; and b. Reviews the contingency plan test/exercise results and initiates corrective actions. Control Enhancements: (1) The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans. (2) The organization tests/exercises the	The organization: a. Tests and/or exercises the contingency plan for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests and/or exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan; and b. Reviews the contingency plan test/exercise results and initiates corrective actions. Control Enhancement: (1) The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related	The organization: a. Tests and/or exercises the contingency plan for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests and/or exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan; and b. Reviews the contingency plan test/exercise results and initiates corrective actions.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations. (4) The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.	plans.	
DCAR-1	CP-5	CONTINGENCY PLAN UPDATE	Withdrawn: Incorporated into CP-2.	Withdrawn: Incorporated into CP-2.	Withdrawn: Incorporated into CP-2.
CODB-2	CP-6	ALTERNATE STORAGE SITE	The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information. Control Enhancements: (1) The organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards. (2) The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives. (3) The organization identifies potential accessibility problems to the alternate	The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information. Control Enhancements: (1) The organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards. (3) The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.		
COAS-1 COEB-1 COSP-1 COSP-2	CP-7	ALTERNATE PROCESSING SITE	The organization: a. Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [*Assignment: organization-defined time period consistent with recovery time objectives*] when the primary processing capabilities are unavailable; and b. Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption. Control Enhancements: (1) The organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards. (2) The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	The organization: a. Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [*Assignment: organization-defined time period consistent with recovery time objectives*] when the primary processing capabilities are unavailable; and b. Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption. Control Enhancements: (1) The organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards. (2) The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			(3) The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements. (4) The organization configures the alternate processing site so that it is ready to be used as the operational site supporting essential missions and business functions. (5) The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.	and outlines explicit mitigation actions. (3) The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements. (5) The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.	
---	CP-8	TELECOMMUNICA-TIONS SERVICES	The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable. Control Enhancements: (1) The organization: (a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements; and (b) Requests Telecommunications	The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable. Control Enhancements: (1) The organization: (a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements; and	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier. (2) The organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services. (3) The organization obtains alternate telecommunications service providers that are separated from primary service providers so as not to be susceptible to the same hazards. (4) The organization requires primary and alternate telecommunications service providers to have contingency plans.	(b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier. (2) The organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.	
CODB-1 CODB-2 COSW-1	CP-9	INFORMATION SYSTEM BACKUP	The organization: a. Conducts backups of user-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; b. Conducts backups of system-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point*	The organization: a. Conducts backups of user-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; b. Conducts backups of system-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and*	The organization: a. Conducts backups of user-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; b. Conducts backups of system-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and*

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			objectives]; c. Conducts backups of information system documentation including security-related documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; and d. Protects the confidentiality and integrity of backup information at the storage location. Control Enhancements: (1) The organization tests backup information [*Assignment: organization-defined frequency*] to verify media reliability and information integrity. (2) The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing. (3) The organization stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not colocated with the operational system.	*recovery point objectives*]; c. Conducts backups of information system documentation including security-related documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; and d. Protects the confidentiality and integrity of backup information at the storage location. Control Enhancement: (1) The organization tests backup information [*Assignment: organization-defined frequency*] to verify media reliability and information integrity.	*recovery point objectives*]; c. Conducts backups of information system documentation including security-related documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; and d. Protects the confidentiality and integrity of backup information at the storage location.
COTR-1 ECND-1	CP-10	INFORMATION SYSTEM RECOVERY AND	The organization provides for the recovery and reconstitution of the information system to a known state	The organization provides for the recovery and reconstitution of the information system to a known state	The organization provides for the recovery and reconstitution of the information system to a known state

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
		RECONSTITUTION	after a disruption, compromise, or failure. Control Enhancements: (2) The information system implements transaction recovery for systems that are transaction-based. (3) The organization provides compensating security controls for organization-defined circumstances that can inhibit recovery and reconstitution. (4) The organization provides the capability to reimage information system components] from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components.	after a disruption, compromise, or failure. Control Enhancements: (2) The information system implements transaction recovery for systems that are transaction-based. (3) The organization provides compensating security controls for organization-defined circumstances that can inhibit recovery and reconstitution. .	after a disruption, compromise, or failure.
Identification and Authentication					
IAIA-1 DCAR-1	IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			identification and authentication policy and associated identification and authentication controls.	identification and authentication policy and associated identification and authentication controls.	the identification and authentication policy and associated identification and authentication controls.
IAIA-1	IA-2	IDENTIFICATION AND AUTHENTICATION (Organizational Users)	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). Control Enhancements: (1) The information system uses multifactor authentication for network access to privileged accounts. (2) The information system uses multifactor authentication for network access to non-privileged accounts. (3) The information system uses multifactor authentication for local access to privileged accounts. (4) The information system uses multifactor authentication for local access to non-privileged accounts. (8) The information system uses [*Assignment: organization-defined replay-resistant authentication mechanisms*] for network access to privileged accounts. (9) The information system uses [*Assignment: organization-defined replay-resistant authentication mechanisms*] for network access to	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). Control Enhancements: (1) The information system uses multifactor authentication for network access to privileged accounts. (2) The information system uses multifactor authentication for network access to non-privileged accounts. (3) The information system uses multifactor authentication for local access to privileged accounts. (8) The information system uses [*Assignment: organization-defined replay-resistant authentication mechanisms*] for network access to privileged accounts.	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). Control Enhancement: (1) The information system uses multifactor authentication for network access to privileged accounts.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			non-privileged accounts.		
---	IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION	The information system uniquely identifies and authenticates [*Assignment: organization-defined list of specific and/or types of devices*] before establishing a connection.	The information system uniquely identifies and authenticates [*Assignment: organization-defined list of specific and/or types of devices*] before establishing a connection.	Not Applicable
IAGA-1 IAIA-1	IA-4	IDENTIFIER MANAGEMENT	The organization manages information system identifiers for users and devices by: a. Receiving authorization from a designated organizational official to assign a user or device identifier; b. Selecting an identifier that uniquely identifies an individual or device; c. Assigning the user identifier to the intended party or the device identifier to the intended device; d. Preventing reuse of user or device identifiers for [*Assignment: organization-defined time period*]; and e. Disabling the user identifier after [*Assignment: organization-defined time period of inactivity*].	The organization manages information system identifiers for users and devices by: a. Receiving authorization from a designated organizational official to assign a user or device identifier; b. Selecting an identifier that uniquely identifies an individual or device; c. Assigning the user identifier to the intended party or the device identifier to the intended device; d. Preventing reuse of user or device identifiers for [*Assignment: organization-defined time period*]; and e. Disabling the user identifier after [*Assignment: organization-defined time period of inactivity*].	The organization manages information system identifiers for users and devices by: a. Receiving authorization from a designated organizational official to assign a user or device identifier; b. Selecting an identifier that uniquely identifies an individual or device; c. Assigning the user identifier to the intended party or the device identifier to the intended device; d. Preventing reuse of user or device identifiers for [*Assignment: organization-defined time period*]; and e. Disabling the user identifier after [*Assignment: organization-defined time period of inactivity*].
IAKM-1 IATS-1	IA-5	AUTHENTICATOR MANAGEMENT	The organization manages information system authenticators for users and devices by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving	The organization manages information system authenticators for users and devices by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device	The organization manages information system authenticators for users and devices by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators upon information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate); g. Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*]; h. Protecting authenticator content from unauthorized disclosure and modification; and i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators. Control Enhancements: (1) The information system, for	receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators upon information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate); g. Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*]; h. Protecting authenticator content from unauthorized disclosure and modification; and i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators. Control Enhancements:	device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators upon information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate); g. Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*]; h. Protecting authenticator content from unauthorized disclosure and modification; and i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			password-based authentication: (a) Enforces minimum password complexity of [*Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type*]; (b) Enforces at least a [*Assignment: organization-defined number of changed characters*] when new passwords are created; (c) Encrypts passwords in storage and in transmission; (d) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; and (e) Prohibits password reuse for [Assignment: organization-defined number] generations. (2) The information system, for PKI-based authentication: (a) Validates certificates by constructing a certification path with status information to an accepted trust anchor; (b) Enforces authorized access to the corresponding private key; and (c) Maps the authenticated identity to the user account. (3) The organization requires that the	(1) The information system, for password-based authentication: (a) Enforces minimum password complexity of [*Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type*]; (b) Enforces at least a [*Assignment: organization-defined number of changed characters*] when new passwords are created; (c) Encrypts passwords in storage and in transmission; (d) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; and (e) Prohibits password reuse for [Assignment: organization-defined number] generations. (2) The information system, for PKI-based authentication: (a) Validates certificates by constructing a certification path with status information to an accepted trust anchor; (b) Enforces authorized access to the corresponding private key; and (c) Maps the authenticated identity to	Control Enhancement: (1) The information system, for password-based authentication: (a) Enforces minimum password complexity of [*Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type*]; (b) Enforces at least a [*Assignment: organization-defined number of changed characters*] when new passwords are created; (c) Encrypts passwords in storage and in transmission; (d) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; and (e) Prohibits password reuse for [Assignment: organization-defined number] generations.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			registration process to receive [*Assignment: organization-defined types of and/or specific authenticators*] be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).	the user account. (3) The organization requires that the registration process to receive [*Assignment: organization-defined types of and/or specific authenticators*] be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).	
---	IA-6	AUTHENTICATOR FEEDBACK	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
---	IA-7	CRYPTOGRAPHIC MODULE AUTHENTICATION	The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.
	IA-8	IDENTIFICATION AND AUTHENTICATION (Non-Organizational Users)	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).
Incident Response					

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
VIIR-1 DCAR-1	IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.
VIIR-1	IR-2	INCIDENT RESPONSE TRAINING	The organization: a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and b. Provides refresher training [*Assignment: organization-defined frequency*]. Control Enhancements: (1) The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations. (2) The organization employs automated mechanisms to provide a	The organization: a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and b. Provides refresher training [*Assignment: organization-defined frequency*].	The organization: a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and b. Provides refresher training [*Assignment: organization-defined frequency*].

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			more thorough and realistic training environment.		
VIIR-1	IR-3	INCIDENT RESPONSE TESTING AND EXERCISES	The organization tests and/or exercises the incident response capability for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests and/or exercises*] to determine the incident response effectiveness and documents the results. Control Enhancement: (1) The organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability.	The organization tests and/or exercises the incident response capability for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests and/or exercises*] to determine the incident response effectiveness and documents the results.	Not Applicable
VIIR-1 E3.3.9	IR-4	INCIDENT HANDLING	The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly. Control Enhancement:	The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.	The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			(1) The organization employs automated mechanisms to support the incident handling process.	Control Enhancement: (1) The organization employs automated mechanisms to support the incident handling process.	
VIIR-1	IR-5	INCIDENT MONITORING	The organization tracks and documents information system security incidents. Control Enhancement: (1) The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.	The organization tracks and documents information system security incidents.	The organization tracks and documents information system security incidents.
VIIR-1 E3.3.9	IR-6	INCIDENT REPORTING	The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within [*Assignment: organization-defined time-period*]; and b. Reports security incident information to designated authorities. Control Enhancement: (1) The organization employs automated mechanisms to assist in the reporting of security incidents.	The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within [*Assignment: organization-defined time-period*]; and b. Reports security incident information to designated authorities. Control Enhancement: (1) The organization employs automated mechanisms to assist in the reporting of security incidents.	The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within [*Assignment: organization-defined time-period*]; and b. Reports security incident information to designated authorities.
---	IR-7	INCIDENT RESPONSE ASSISTANCE	The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and	The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and	The organization provides an incident response support resource, integral to the organizational incident response capability, that

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			assistance to users of the information system for the handling and reporting of security incidents. Control Enhancement: (1) The organization employs automated mechanisms to increase the availability of incident response-related information and support.	assistance to users of the information system for the handling and reporting of security incidents. Control Enhancement: (1) The organization employs automated mechanisms to increase the availability of incident response-related information and support.	offers advice and assistance to users of the information system for the handling and reporting of security incidents.
	IR-8	INCIDENT RESPONSE PLAN	The organization: a. Develops an incident response plan that: - Provides the organization with a roadmap for implementing its incident response capability; - Describes the structure and organization of the incident response capability; - Provides a high-level approach for how the incident response capability fits into the overall organization; - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; - Defines reportable incidents; - Provides metrics for measuring the incident response capability within the organization. - Defines the resources and management support needed to effectively maintain and mature an incident response capability; and	The organization: a. Develops an incident response plan that: - Provides the organization with a roadmap for implementing its incident response capability; - Describes the structure and organization of the incident response capability; - Provides a high-level approach for how the incident response capability fits into the overall organization; - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; - Defines reportable incidents; - Provides metrics for measuring the incident response capability within the organization. - Defines the resources and management support needed to effectively maintain and mature an	The organization: a. Develops an incident response plan that: - Provides the organization with a roadmap for implementing its incident response capability; - Describes the structure and organization of the incident response capability; - Provides a high-level approach for how the incident response capability fits into the overall organization; - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; - Defines reportable incidents; - Provides metrics for measuring the incident response capability within the organization. - Defines the resources and management support needed to effectively maintain and mature an

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			- Is reviewed and approved by designated officials within the organization; b. Distributes copies of the incident response plan to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*]; c. Reviews the incident response plan [*Assignment: organization-defined frequency*]; d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and e. Communicates incident response plan changes to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*].	incident response capability; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the incident response plan to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*]; c. Reviews the incident response plan [*Assignment: organization-defined frequency*]; d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and e. Communicates incident response plan changes to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*].	incident response capability; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the incident response plan to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*]; c. Reviews the incident response plan [*Assignment: organization-defined frequency*]; d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and e. Communicates incident response plan changes to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*].
Maintenance					
PRMP-1 DCAR-1	MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented information system maintenance policy that	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented information system maintenance policy that	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented information system maintenance policy that

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls. .
---	MA-2	CONTROLLED MAINTENANCE	The organization: (a) schedules, performs, documents and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; (b) controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; (c) requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; (d) sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and (e) checks all potentially impacted security controls to verify that the controls are still functioning properly	The organization: (a) schedules, performs, documents and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; (b) controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; (c) requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; (d) sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and (e) checks all potentially impacted security controls to verify that the controls are still functioning	The organization: (a) schedules, performs, documents and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; (b) controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; (c) requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; (d) sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			following maintenance or repair actions. (1) Control Enhancements: The organization maintains maintenance records for the information system that include: (a) Date and time of maintenance; (b) Name of the individual performing the maintenance; (c) Name of escort, if necessary; (d) A description of the maintenance performed; and (e) A list of equipment removed or replaced (including identification numbers, if applicable). (2) The organization employs automated mechanisms to schedule, conduct, and document maintenance and repairs as required, producing up-to date, accurate, complete, and available records of all maintenance and repair actions, needed, in process, and completed.	properly following maintenance or repair actions. (1) Control Enhancements: The organization maintains maintenance records for the information system that include: (a) Date and time of maintenance; (b) Name of the individual performing the maintenance; (c) Name of escort, if necessary; (d) A description of the maintenance performed; and (e) A list of equipment removed or replaced (including identification numbers, if applicable).	maintenance or repairs; and (e) checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.
---	MA-3	MAINTENANCE TOOLS	The organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools. Control Enhancements: (1) The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious	The organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools. Control Enhancements: (1) The organization inspects all maintenance tools carried into a facility by maintenance personnel for	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			improper modifications. Maintenance tools include, for example, diagnostic and test equipment used to conduct maintenance on the information system. (2) The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system. (3) The organization prevents the unauthorized removal of maintenance equipment by one of the following: (i) verifying that there is no organizational information contained on the equipment; (ii) sanitizing or destroying the equipment; (iii) retaining the equipment within the facility; or (iv) obtaining an exemption from a designated organization official explicitly authorizing removal of the equipment from the facility.	obvious improper modifications. Maintenance tools include, for example, diagnostic and test equipment used to conduct maintenance on the information system. (2) The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.	
EBRP-1	MA-4	NON-LOCAL MAINTENANCE	The organization: a. Authorizes, monitors, and controls non-local maintenance and diagnostic activities; b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;	The organization: a. Authorizes, monitors, and controls non-local maintenance and diagnostic activities; b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;	The organization: a. Authorizes, monitors, and controls non-local maintenance and diagnostic activities; b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong identification and authentication techniques in the establishment of non-local

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			d. Maintains records for non-local maintenance and diagnostic activities; and e. Terminates all sessions and network connections when non-local maintenance is completed. Control Enhancements: (1) The organization audits non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions. (2) The organization documents, in the security plan for the information (3) The organization: (a) Requires that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or (b) Removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants)	d. Maintains records for non-local maintenance and diagnostic activities; and e. Terminates all sessions and network connections when non-local maintenance is completed. Control Enhancements: (1) The organization audits non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions. (2) The organization documents, in the security plan for the information	maintenance and diagnostic sessions; d. Maintains records for non-local maintenance and diagnostic activities; and e. Terminates all sessions and network connections when non-local maintenance is completed.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			before reconnecting the component to the information system.		
PRMP-1	MA-5	MAINTENANCE PERSONNEL	The organization: a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.	The organization: a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.	The organization: a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.
COMS-1 COSP-1	MA-6	TIMELY MAINTENANCE	The organization obtains maintenance support and/or spare parts for [*Assignment: organization-defined list of security-critical information system components and/or key information technology components*] within [*Assignment: organization-defined time period*] of failure.	The organization obtains maintenance support and/or spare parts for [*Assignment: organization-defined list of security-critical information system components and/or key information technology components*] within [*Assignment: organization-defined time period*] of failure.	Not Applicable
Media Protection					

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
PESP-1 DCAR-1	MP-1	MEDIA PROTECTION POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.
PEDI-1 PEPF-1	MP-2	MEDIA ACCESS	The organization restricts access to [Assignment: organization-defined types of digital and non-digital media] to [Assignment: organization-defined list of authorized individuals] using [Assignment: organization-defined security measures]. Control Enhancement: (1) The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.	The organization restricts access to [Assignment: organization-defined types of digital and non-digital media] to [Assignment: organization-defined list of authorized individuals] using [Assignment: organization-defined security measures]. Control Enhancement: (1) The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.	The organization restricts access to [Assignment: organization-defined types of digital and non-digital media] to [Assignment: organization-defined list of authorized individuals] using [Assignment: organization-defined security measures].
ECML-1	MP-3	MEDIA MARKING	The organization: a. Marks, in accordance with	The organization: a. Marks, in accordance with	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts [*Assignment: organization-defined list of removable media types*] from marking as long as the exempted items remain within [*Assignment: organization-defined controlled areas*].	organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts [*Assignment: organization-defined list of removable media types*] from marking as long as the exempted items remain within [*Assignment: organization-defined controlled areas*].	
PESS-1	MP-4	MEDIA STORAGE	The organization: a. Physically controls and securely stores [*Assignment: organization-defined types of digital and non-digital media*] within [*Assignment: organization-defined controlled areas*] using [*Assignment: organization-defined security measures*]; b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	The organization: a. Physically controls and securely stores [*Assignment: organization-defined types of digital and non-digital media*] within [*Assignment: organization-defined controlled areas*] using [*Assignment: organization-defined security measures*]; b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	Not Applicable
---	MP-5	MEDIA TRANSPORT	The organization: a. Protects and controls [*Assignment: organization-defined types of digital and non-digital media*] during transport outside of controlled areas using [*Assignment: organization-defined*	The organization: a. Protects and controls [*Assignment: organization-defined types of digital and non-digital media*] during transport outside of controlled areas using [*Assignment: organization-*	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			security measures]; b. Maintains accountability for information system media during transport outside of controlled areas; and c. Restricts the activities associated with transport of such media to authorized personnel. Control Enhancements: (2) The organization documents activities associated with the transport of information system media. (3) The organization employs an identified custodian throughout the transport of information system media. (4) The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	*defined security measures*]; b. Maintains accountability for information system media during transport outside of controlled areas; and c. Restricts the activities associated with transport of such media to authorized personnel. Control Enhancements: (2) The organization documents activities associated with the transport of information system media. (4) The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	
PECS-1 PEDD-1	MP-6	MEDIA SANITIZATION	The organization sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse. Control Enhancements: (1) The organization tracks, documents, and verifies media sanitization and disposal actions. (2) The organization tests sanitization	The organization sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse.	The organization sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			equipment and procedures to verify correct performance [*Assignment: organization-defined frequency*]. (3) The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: [*Assignment: organization-defined list of circumstances requiring sanitization of portable, removable storage devices*].		
PEDD-1	MP-7	MEDIA DESTRUCTION AND DISPOSAL	Withdrawn from SP 800-53, Rev. 3	Withdrawn from SP 800-53, Rev. 3	Withdrawn from SP 800-53, Rev. 3
Physical and Environmental Protection					
PETN-1 DCAR-1	PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
PECF-1	PE-2	PHYSICAL ACCESS AUTHORIZATIONS	The organization: a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); b. Issues authorization credentials; c. Reviews and approves the access list and authorization credentials [*Assignment: organization-defined frequency*], removing from the access list personnel no longer requiring access.	The organization: a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); b. Issues authorization credentials; c. Reviews and approves the access list and authorization credentials [*Assignment: organization-defined frequency*], removing from the access list personnel no longer requiring access.	The organization: a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); b. Issues authorization credentials; c. Reviews and approves the access list and authorization credentials [*Assignment: organization-defined frequency*], removing from the access list personnel no longer requiring access.
PEPF-1	PE-3	PHYSICAL ACCESS CONTROL	The organization: a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible); b. Verifies individual access authorizations before granting access to the facility; c. Controls entry to the facility containing the information system using physical access devices and/or guards; d. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk; e. Secures keys, combinations, and	The organization: a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible); b. Verifies individual access authorizations before granting access to the facility; c. Controls entry to the facility containing the information system using physical access devices and/or guards; d. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;	The organization: a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible); b. Verifies individual access authorizations before granting access to the facility; c. Controls entry to the facility containing the information system using physical access devices and/or guards; d. Controls access to areas officially designated as publicly accessible in accordance with the organization's

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			other physical access devices; f. Inventories physical access devices [*Assignment: organization-defined frequency*]; and g. Changes combinations and keys [*Assignment: organization-defined frequency*] and when keys are lost, combinations are compromised, or individuals are transferred or terminated. Control Enhancements: (1) The organization enforces physical access authorizations to the information system independent of the physical access controls for the facility.	e. Secures keys, combinations, and other physical access devices; f. Inventories physical access devices [*Assignment: organization-defined frequency*]; and g. Changes combinations and keys [*Assignment: organization-defined frequency*] and when keys are lost, combinations are compromised, or individuals are transferred or terminated.	assessment of risk; e. Secures keys, combinations, and other physical access devices; f. Inventories physical access devices [*Assignment: organization-defined frequency*]; and g. Changes combinations and keys [*Assignment: organization-defined frequency*] and when keys are lost, combinations are compromised, or individuals are transferred or terminated.
	PE-4	ACCESS CONTROL FOR TRANSMISSION MEDIUM	The organization controls physical access to information system distribution and transmission lines within organizational facilities.	The organization controls physical access to information system distribution and transmission lines within organizational facilities.	Not Applicable
PEDI-1 PEPF-1	PE-5	ACCESS CONTROL FOR OUTPUT DEVICES	The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	Not Applicable
PEPF-2	PE-6	MONITORING PHYSICAL ACCESS	The organization: a. Monitors physical access to the information system to detect and respond to physical security incidents; b. Reviews physical access logs [*Assignment: organization-defined frequency*]; and	The organization: a. Monitors physical access to the information system to detect and respond to physical security incidents; b. Reviews physical access logs [*Assignment: organization-defined frequency*]; and	The organization: a. Monitors physical access to the information system to detect and respond to physical security incidents; b. Reviews physical access logs [*Assignment: organization-defined*

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			c. Coordinates results of reviews and investigations with the organization's incident response capability. Control Enhancements: (1) The organization monitors real-time physical intrusion alarms and surveillance equipment. (2) The organization employs automated mechanisms to recognize potential intrusions and initiate designated response actions.	c. Coordinates results of reviews and investigations with the organization's incident response capability. Control Enhancements: (1) The organization monitors real-time physical intrusion alarms and surveillance equipment.	*frequency*]; and c. Coordinates results of reviews and investigations with the organization's incident response capability.
PEVC-1	PE-7	VISITOR CONTROL	The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible. Control Enhancement: (1) The organization escorts visitors and monitors visitor activity, when required.	The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible. Control Enhancement: (1) The organization escorts visitors and monitors visitor activity, when required.	The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.
PEPF-2 PEVC-1	PE-8	ACCESS RECORDS	The organization: a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and b. Reviews visitor access records	The organization: a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and	The organization: a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			[*Assignment: organization-defined frequency*]. Control Enhancements: (1) The organization employs automated mechanisms to facilitate the maintenance and review of access records. (2) The organization maintains a record of all physical access, both visitor and authorized individuals.	b. Reviews visitor access records [*Assignment: organization-defined frequency*].	b. Reviews visitor access records [*Assignment: organization-defined frequency*].
---	PE-9	POWER EQUIPMENT AND POWER CABLING	The organization protects power equipment and power cabling for the information system from damage and destruction.	The organization protects power equipment and power cabling for the information system from damage and destruction.	Not Applicable
PEMS-1	PE-10	EMERGENCY SHUTOFF	The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in [*Assignment: organization-defined location by information system or system component*] to facilitate safe and easy access for personnel; and c. Protects emergency power shutoff capability from unauthorized activation.	The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in [*Assignment: organization-defined location by information system or system component*] to facilitate safe and easy access for personnel; and c. Protects emergency power shutoff capability from unauthorized activation.	Not Applicable
COPS-1	PE-11	EMERGENCY	The organization provides a short-term uninterruptible power supply to facilitate	The organization provides a short-term uninterruptible power supply to	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
COPS-2 COPS-3		POWER	an orderly shutdown of the information system in the event of a primary power source loss. Control Enhancement: (1) The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.	facilitate an orderly shutdown of the information system in the event of a primary power source loss.	
PEEL-1	PE-12	EMERGENCY LIGHTING	The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.
PEFD-1 PEFS-1	PE-13	FIRE PROTECTION	The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source. Control Enhancements: (1) The organization employs fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire. (2) The organization employs fire	The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source. Control Enhancements: (1) The organization employs fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire. (2) The organization employs fire	The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders. (3) The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.	suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders. (3) The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.	
PEHC-1 PETC-1	PE-14	TEMPERATURE AND HUMIDITY CONTROLS	The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at [*Assignment: organization-defined acceptable levels*]; and b. Monitors temperature and humidity levels [*Assignment: organization-defined frequency*].	The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at [*Assignment: organization-defined acceptable levels*]; and b. Monitors temperature and humidity levels [*Assignment: organization-defined frequency*].	The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at [*Assignment: organization-defined acceptable levels*]; and b. Monitors temperature and humidity levels [*Assignment: organization-defined frequency*].
---	PE-15	WATER DAMAGE PROTECTION	The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel. Control Enhancement: (1) The organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a water leak.	The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.	The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
---	PE-16	DELIVERY AND REMOVAL	The organization authorizes, monitors, and controls [*Assignment: organization-defined types of information system components*] entering and exiting the facility and maintains records of those items.	The organization authorizes, monitors, and controls [*Assignment: organization-defined types of information system components*] entering and exiting the facility and maintains records of those items.	The organization authorizes, monitors, and controls [*Assignment: organization-defined types of information system components*] entering and exiting the facility and maintains records of those items.
EBRU-1	PE-17	ALTERNATE WORK SITE	The organization: a. Employs [*Assignment: organization-defined management, operational, and technical information system security controls*] at alternate work sites; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.	The organization: a. Employs [*Assignment: organization-defined management, operational, and technical information system security controls*] at alternate work sites; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.	Not Applicable
	PE-18	LOCATION OF INFORMATION SYSTEM COMPONENTS	The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. Control Enhancements: (1) The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the	The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			physical and environmental hazards in its risk mitigation strategy.		
	PE-19	INFORMATION LEAKAGE	Not Applicable	Not Applicable	Not Applicable
Planning					
DCAR-1 E3.4.6	PL-1	SECURITY PLANNING POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.
DCSD-1	PL-2	SYSTEM SECURITY PLAN	The organization: a. Develops a security plan for the information system that: - Is consistent with the organization's enterprise architecture; - Explicitly defines the authorization boundary for the system; - Describes the operational context of the information system in terms of	The organization: a. Develops a security plan for the information system that: - Is consistent with the organization's enterprise architecture; - Explicitly defines the authorization boundary for the system; - Describes the operational context of the information system in terms of	The organization: a. Develops a security plan for the information system that: - Is consistent with the organization's enterprise architecture; - Explicitly defines the authorization boundary for the system; - Describes the operational context

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			missions and business processes; - Provides the security category and impact level of the information system including supporting rationale; - Describes the operational environment for the information system; - Describes relationships with or connections to other information systems; - Provides an overview of the security requirements for the system; - Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and - Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Reviews the security plan for the information system [*Assignment: organization-defined frequency*]; and c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.	missions and business processes; - Provides the security category and impact level of the information system including supporting rationale; - Describes the operational environment for the information system; - Describes relationships with or connections to other information systems; - Provides an overview of the security requirements for the system; - Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and - Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Reviews the security plan for the information system [*Assignment: organization-defined frequency*]; and c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.	of the information system in terms of missions and business processes; - Provides the security category and impact level of the information system including supporting rationale; - Describes the operational environment for the information system; - Describes relationships with or connections to other information systems; - Provides an overview of the security requirements for the system; - Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and - Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Reviews the security plan for the information system [*Assignment: organization-defined frequency*]; and c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
					implementation or security control assessments.
5.7.5	PL-3	SYSTEM SECURITY PLAN UPDATE	Withdrawn: Incorporated into PL-2.	Withdrawn: Incorporated into PL-2.	Withdrawn: Incorporated into PL-2.
5.7.5 PRRB-1	PL-4	RULES OF BEHAVIOR	The organization: a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.	The organization: a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.	The organization: a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.
---	PL-5	PRIVACY IMPACT ASSESSMENT	The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.	The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.	The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.
	PL-6	SECURITY-RELATED ACTIVITY PLANNING	The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.	The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets,	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
				and individuals.	
Personnel Security					
PRRB-1 DCAR-1	PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.
---	PS-2	POSITION CATEGORIZATION	The organization: a. Assigns a risk designation to all positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and revises position risk designations [*Assignment: organization-defined frequency*].	The organization: a. Assigns a risk designation to all positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and revises position risk designations [*Assignment: organization-defined frequency*].	The organization: a. Assigns a risk designation to all positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and revises position risk designations [*Assignment: organization-defined frequency*].
PRAS-1	PS-3	PERSONNEL SCREENING	The organization: a. Screens individuals prior to authorizing access to the information system; and	The organization: a. Screens individuals prior to authorizing access to the information system; and	The organization: a. Screens individuals prior to authorizing access to the information system; and

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			b. Rescreens individuals according to [*Assignment: organization-defined list of conditions requiring rescreening and, where re-screening is so indicated, the frequency of such rescreening*].	b. Rescreens individuals according to [*Assignment: organization-defined list of conditions requiring rescreening and, where re-screening is so indicated, the frequency of such rescreening*].	b. Rescreens individuals according to [*Assignment: organization-defined list of conditions requiring rescreening and, where re-screening is so indicated, the frequency of such rescreening*].
5.12.7	PS-4	PERSONNEL TERMINATION	The organization, upon termination of individual employment: a. Terminates information system access; b. Conducts exit interviews; c. Retrieves all security-related organizational information system-related property; and d. Retains access to organizational information and information systems formerly controlled by terminated individual.	The organization, upon termination of individual employment: a. Terminates information system access; b. Conducts exit interviews; c. Retrieves all security-related organizational information system-related property; and d. Retains access to organizational information and information systems formerly controlled by terminated individual.	The organization, upon termination of individual employment: a. Terminates information system access; b. Conducts exit interviews; c. Retrieves all security-related organizational information system-related property; and d. Retains access to organizational information and information systems formerly controlled by terminated individual.
5.12.7	PS-5	PERSONNEL TRANSFER	The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates [*Assignment: organization-defined transfer or reassignment actions*] within [*Assignment: organization-defined time period following the formal transfer action*].	The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates [*Assignment: organization-defined transfer or reassignment actions*] within [*Assignment: organization-defined time period following the formal transfer action*].	The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates [*Assignment: organization-defined transfer or reassignment actions*] within [*Assignment: organization-defined time period following the formal transfer action*].
PRRB-1	PS-6	ACCESS AGREEMENTS	The organization: a. Ensures that individuals requiring	The organization: a. Ensures that individuals requiring	The organization: a. Ensures that individuals requiring

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			access to organizational information and information systems sign appropriate access agreements prior to being granted access; and b. Reviews/updates the access agreements [*Assignment: organization-defined frequency*].	access to organizational information and information systems sign appropriate access agreements prior to being granted access; and b. Reviews/updates the access agreements [*Assignment: organization-defined frequency*].	access to organizational information and information systems sign appropriate access agreements prior to being granted access; and b. Reviews/updates the access agreements [*Assignment: organization-defined frequency*].
5.7.10	PS-7	THIRD-PARTY PERSONNEL SECURITY	The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Documents personnel security requirements; and c. Monitors provider compliance.	The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Documents personnel security requirements; and c. Monitors provider compliance.	The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Documents personnel security requirements; and c. Monitors provider compliance.
PRRB-1	PS-8	PERSONNEL SANCTIONS	The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.	The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.	The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.
Risk Assessment					
DCAR-1	RA-1	RISK ASSESSMENT POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	compliance; and b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	compliance; and b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.
E3.4.2	RA-2	SECURITY CATEGORIZATION	The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.
DCDS-1 DCII-1 E3.3.10	RA-3	RISK ASSESSMENT	The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in [*Selection: security plan; risk*	The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results	The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			assessment report; [*Assignment: organization-defined document*]]; c. Reviews risk assessment results [*Assignment: organization-defined frequency*]; and d. Updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.	in [*Selection: security plan; risk assessment report;* [*Assignment: organization-defined document*]]; c. Reviews risk assessment results [*Assignment: organization-defined frequency*]; and d. Updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.	results in [*Selection: security plan; risk assessment report;* [*Assignment: organization-defined document*]]; c. Reviews risk assessment results [*Assignment: organization-defined frequency*]; and d. Updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.
DCAR-1 DCII-1	RA-4	RISK ASSESSMENT UPDATE	Withdrawn: Incorporated into RA-3.	Withdrawn: Incorporated into RA-3.	Withdrawn: Incorporated into RA-3.
ECMT-1 VIVM-1	RA-5	VULNERABILITY SCANNING	The organization: a. Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that promote	The organization: a. Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that promote	The organization: a. Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that promote

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			interoperability among tools and automate parts of the vulnerability management process by using standards for: - Enumerating platforms, software flaws, and improper configurations; - Formatting and making transparent, checklists and test procedures; and - Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). Control Enhancements: (1) The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned. (2) The organization updates the list of	interoperability among tools and automate parts of the vulnerability management process by using standards for: - Enumerating platforms, software flaws, and improper configurations; - Formatting and making transparent, checklists and test procedures; and - Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). Control Enhancements: (1) The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.	interoperability among tools and automate parts of the vulnerability management process by using standards for: - Enumerating platforms, software flaws, and improper configurations; - Formatting and making transparent, checklists and test procedures; and - Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			information system vulnerabilities scanned [*Assignment: organization-defined frequency*] or when new vulnerabilities are identified and reported. (3) The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked). (4) The organization attempts to discern what information about the information system is discoverable by adversaries. (5) The organization includes privileged access authorization to [*Assignment: organization-identified information system components*] for selected vulnerability scanning activities to facilitate more thorough scanning. (7) The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to detect the presence of unauthorized software on organizational information systems and notify designated organizational officials.		
System and Services Acquisition					
DCAR-1	SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
		PROCEDURES	a. A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	a. A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	a. A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.
DCPB-1 E3.3.4	SA-2	ALLOCATION OF RESOURCES	The organization: a. Includes a determination of information security requirements for the information system in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.	The organization: a. Includes a determination of information security requirements for the information system in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.	The organization: a. Includes a determination of information security requirements for the information system in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.
5.8.1	SA-3	LIFE CYCLE SUPPORT	The organization: a. Manages the information system using a system development life cycle methodology that includes information	The organization: a. Manages the information system using a system development life cycle methodology that includes information	The organization: a. Manages the information system using a system development life cycle methodology that includes

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			security considerations; b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and c. Identifies individuals having information system security roles and responsibilities.	security considerations; b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and c. Identifies individuals having information system security roles and responsibilities.	information security considerations; b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and c. Identifies individuals having information system security roles and responsibilities.
DCAS-1 DCDS-1 DCIT-1 DCMC-1	SA-4	ACQUISITIONS	The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards: a. Security functional requirements/specifications; b. Security-related documentation requirements; and c. Developmental and evaluation-related assurance requirements. Control Enhancements: (1) The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.	The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards: a. Security functional requirements/specifications; b. Security-related documentation requirements; and c. Developmental and evaluation-related assurance requirements. Control Enhancements: (1) The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or	The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards: a. Security functional requirements/specifications; b. Security-related documentation requirements; and c. Developmental and evaluation-related assurance requirements.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			(2) The organization requires in acquisition documents that vendors/contractors provide information describing the design and implementation details of the security controls to be employed within the information system, information system components, or information system services (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls. (4) The organization ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.	(4) The organization ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.	
DCCS-1 DCHW-1 DCID-1 DCSD-1 DCSW-1 ECND-1 DCFA-1	SA-5	INFORMATION SYSTEM DOCUMENTATION	The organization: a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes: - Secure configuration, installation, and operation of the information system; - Effective use and maintenance of security features/functions; and - Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and b. Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:	The organization: a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes: - Secure configuration, installation, and operation of the information system; - Effective use and maintenance of security features/functions; and - Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and b. Obtains, protects as required, and makes available to authorized	The organization: a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes: - Secure configuration, installation, and operation of the information system; - Effective use and maintenance of security features/functions; and - Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and b. Obtains, protects as required, and makes available to authorized

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			- User-accessible security features/functions and how to effectively use those security features/functions; - Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and User responsibilities in maintaining the security of the information and information system; and c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent. Control Enhancements: (1) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing. (2) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the security-relevant external interfaces to the information system with sufficient detail to permit analysis and testing. (3) The organization obtains, protects	personnel, user documentation for the information system that describes: - User-accessible security features/functions and how to effectively use those security features/functions; - Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and User responsibilities in maintaining the security of the information and information system; and c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent. Control Enhancements: (1) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing. (3) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation	personnel, user documentation for the information system that describes: - User-accessible security features/functions and how to effectively use those security features/functions; - Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and - User responsibilities in maintaining the security of the information and information system; and c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.	that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.	
DCPD-1	SA-6	SOFTWARE USAGE RESTRICTIONS	The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.
---	SA-7	USER INSTALLED SOFTWARE	The organization enforces explicit rules governing the installation of software by users.	The organization enforces explicit rules governing the installation of software by users.	The organization enforces explicit rules governing the installation of software by users.
DCBP-1 DCCS-1	SA-8	SECURITY DESIGN PRINCIPLES	The organization applies information system security engineering principles in the specification, design,	The organization applies information system security engineering principles in the specification, design,	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
E3.4.4			development, implementation, and modification of the information system.	development, implementation, and modification of the information system.	
DCDS-1 DCID-1 DCIT-1 DCPP-1	SA-9	EXTERNAL INFORMATION SYSTEM SERVICES	The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Monitors security control compliance by external service providers.	The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Monitors security control compliance by external service providers.	The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Monitors security control compliance by external service providers.
---	SA-10	DEVELOPER CONFIGURATION MANAGEMENT	The organization requires that information system developers/integrators: a. Perform configuration management during information system design, development, implementation, and operation; b. Manage and control changes to the information system; c. Implement only organization-approved changes;	The organization requires that information system developers/integrators: a. Perform configuration management during information system design, development, implementation, and operation; b. Manage and control changes to the information system; c. Implement only organization-approved changes;	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			d. Document approved changes to the information system; and e. Track security flaws and flaw resolution.	d. Document approved changes to the information system; and e. Track security flaws and flaw resolution.	
E3.4.4	SA-11	DEVELOPER SECURITY TESTING	The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers): a. Create and implement a security test and evaluation plan; b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and c. Document the results of the security testing/evaluation and flaw remediation processes.	The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers): a. Create and implement a security test and evaluation plan; b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and c. Document the results of the security testing/evaluation and flaw remediation processes.	Not Applicable
	SA-12	SUPPLY CHAIN PROTECTION	The organization protects against supply chain threats by employing: [*Assignment: organization-defined list of measures to protect against supply chain threats*] as part of a comprehensive, defense-in-breadth information security strategy.	Not Applicable	Not Applicable
	SA-13	TRUSTWORTHI-NESS	The organization requires that the information system meets [*Assignment: organization-defined level of trustworthiness*].	Not Applicable	Not Applicable
	SA-14	CRITICAL INFORMATION	Not Applicable	Not Applicable	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
		SYSTEM COMPONENTS			
System and Communications Protection					
DCAR-1	SC-1	SYSTEM AND COMMUNICA-TIONS PROTECTION POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.
DCPA-1	SC-2	APPLICATION PARTITIONING	The information system separates user functionality (including user interface services) from information system management functionality.	The information system separates user functionality (including user interface services) from information system management functionality.	Not Applicable
DCSP-1	SC-3	SECURITY FUNCTION ISOLATION	The information system isolates security functions from nonsecurity functions.	Not Applicable	Not Applicable
ECRC-1	SC-4	INFORMATION IN SHARED RESOURCES	The information system prevents unauthorized and unintended information transfer via shared system	The information system prevents unauthorized and unintended information transfer via shared	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			resources.	system resources.	
---	SC-5	DENIAL OF SERVICE PROTECTION	The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined list of types of denial of service attacks or reference to source for current list*].	The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined list of types of denial of service attacks or reference to source for current list*].	The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined list of types of denial of service attacks or reference to source for current list*].
---	SC-6	RESOURCE PRIORITY	Not Applicable	Not Applicable	Not Applicable
COEB-1 EBBD-1 ECIM-1 ECVI-1	SC-7	BOUNDARY PROTECTION	The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and b. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. Control Enhancements: (1) The organization physically allocates publicly accessible information system components to separate subnetworks with separate physical network interfaces. (2) The information system prevents public access into the organization's	The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and b. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. Control Enhancements: (1) The organization physically allocates publicly accessible information system components to separate subnetworks with separate physical network interfaces. (2) The information system prevents public access into the organization's	The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and b. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			internal networks except as appropriately mediated by managed interfaces employing boundary protection devices. (3) The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic. (4) The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; (e) Reviews exceptions to the traffic flow policy [*Assignment: organization-defined frequency*]; and (f) Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need. (5) The information system at managed interfaces, denies network traffic by	internal networks except as appropriately mediated by managed interfaces employing boundary protection devices. (3) The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic. (4) The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; (e) Reviews exceptions to the traffic flow policy [*Assignment: organization-defined frequency*]; and (f) Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need. (5) The information system at	

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			default and allows network traffic by exception (i.e., deny all, permit by exception). (6) The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms. (7) The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks. (8) The information system routes [*Assignment: organization-defined internal communications traffic*] to [*Assignment: organization-defined external networks*] through authenticated proxy servers within the managed interfaces of boundary protection devices.	managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception). (7) The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.	
ECTM-1	SC-8	TRANSMISSION INTEGRITY	The information system protects the integrity of transmitted information. Control Enhancements: (1) The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected	The information system protects the integrity of transmitted information. Control Enhancements: (1) The organization employs cryptographic mechanisms to recognize changes to information	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			by alternative physical measures.	during transmission unless otherwise protected by alternative physical measures.	
ECCT-1	SC-9	TRANSMISSION CONFIDENTIALITY	The information system protects the confidentiality of transmitted information. Control Enhancement: (1) The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.	The information system protects the confidentiality of transmitted information. Control Enhancement: (1) The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.	Not Applicable
---	SC-10	NETWORK DISCONNECT	The information system terminates the network connection associated with a communications session at the end of the session or after [*Assignment: organization-defined time period*] of inactivity.	The information system terminates the network connection associated with a communications session at the end of the session or after [*Assignment: organization-defined time period*] of inactivity.	Not Applicable
	SC-11	TRUSTED PATH	Not Applicable	Not Applicable	Not Applicable
IAKM-1	SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	The organization establishes and manages cryptographic keys for required cryptography employed within the information system. Control Enhancement: (1) The organization maintains availability of information in the event of the loss of cryptographic keys by users.	The organization establishes and manages cryptographic keys for required cryptography employed within the information system.	The organization establishes and manages cryptographic keys for required cryptography employed within the information system.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
IAKM-1 IATS-1	SC-13	USE OF CRYPTOGRAPHY	The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
EBPW-1	SC-14	PUBLIC ACCESS PROTECTIONS	The information system protects the integrity and availability of publicly available information and applications.	The information system protects the integrity and availability of publicly available information and applications.	The information system protects the integrity and availability of publicly available information and applications.
ECVI-1	SC-15	COLLABORATIVE COMPUTING DEVICES	The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: [*Assignment: organization-defined exceptions where remote activation is to be allowed*]; and b. Provides an explicit indication of use to users physically present at the devices.	The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: [*Assignment: organization-defined exceptions where remote activation is to be allowed*]; and b. Provides an explicit indication of use to users physically present at the devices.	The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: [*Assignment: organization-defined exceptions where remote activation is to be allowed*]; and b. Provides an explicit indication of use to users physically present at the devices.
	SC-16	TRANSMISSION OF SECURITY ATTRIBUTES	Not Applicable	Not Applicable	Not Applicable
IAKM-1	SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.	The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
DCMC-1	SC-18	MOBILE CODE	The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system.	The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system.	Not Applicable
ECVI-1	SC-19	VOICE OVER INTERNET PROTOCOL	The organization: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of VoIP within the information system.	The organization: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of VoIP within the information system.	Not Applicable
	SC-20	SECURE NAME / ADDRESS RESOLUTION SERVICE (Authoritative Source)	The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries. Control Enhancements: (1) The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child	The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries. Control Enhancements: (1) The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child	The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries. Control Enhancements: (1) The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			supports secure resolution services) enable verification of a chain of trust among parent and child domains.	supports secure resolution services) enable verification of a chain of trust among parent and child domains.	child supports secure resolution services) enable verification of a chain of trust among parent and child domains.
	SC-21	SECURE NAME / ADDRESS RESOLUTION SERVICE (Recursive or Caching Resolver)	The information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems.	Not Applicable	Not Applicable
	SC-22	ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE	The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.	The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.	Not Applicable
	SC-23	SESSION AUTHENTICITY	The information system provides mechanisms to protect the authenticity of communications sessions.	The information system provides mechanisms to protect the authenticity of communications sessions.	Not Applicable
	SC-24	FAIL IN KNOWN STATE	The information system fails to a [*Assignment: organization-defined known-state*] for [*Assignment: organization-defined types of failures*] preserving [*Assignment: organization-defined system state information*] in failure.	Not Applicable	Not Applicable
	SC-25	THIN NODES	Not Applicable	Not Applicable	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
	SC-26	HONEYPOTS	Not Applicable	Not Applicable	Not Applicable
	SC-27	OPERATING SYSTEM-INDEPENDENT APPLICATIONS	Not Applicable	Not Applicable	Not Applicable
	SC-28	PROTECTION OF INFORMATION AT REST	The information system protects the confidentiality and integrity of information at rest.	The information system protects the confidentiality and integrity of information at rest.	Not Applicable
	SC-29	HETEROGENEITY	Not Applicable	Not Applicable	Not Applicable
	SC-30	VIRTUALIZATION TECHNIQUES	Not Applicable	Not Applicable	Not Applicable
	SC-31	COVERT CHANNEL ANALYSIS	Not Applicable	Not Applicable	Not Applicable
	SC-32	INFORMATION SYSTEM PARTITIONING	The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.	The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.	Not Applicable
	SC-33	TRANSMISSION PREPARATION INTEGRITY	Not Applicable	Not Applicable	Not Applicable
	SC-34	NON-MODIFIABLE EXECUTABLE PROGRAMS	Not Applicable	Not Applicable	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
System and Information Integrity					
DCAR-1	SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.
DCSQ-1 DCCT-1 E.3.3.5.7	SI-2	FLAW REMEDIATION	The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and c. Incorporates flaw remediation into the organizational configuration management process. Control Enhancements: (1) The organization centrally manages the flaw remediation process and installs software updates automatically.	The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and c. Incorporates flaw remediation into the organizational configuration management process. Control Enhancement: (2) The organization employs automated mechanisms [*Assignment:*	The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and c. Incorporates flaw remediation into the organizational configuration management process.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			(2) The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to determine the state of information system components with regard to flaw remediation.	*organization-defined frequency*] to determine the state of information system components with regard to flaw remediation.	
ECVP-1 VIVM-1	SI-3	MALICIOUS CODE PROTECTION	The organization: a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: - Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or - Inserted through the exploitation of information system vulnerabilities; b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: - Perform periodic scans of the information system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and	The organization: a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: - Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or - Inserted through the exploitation of information system vulnerabilities; b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: - Perform periodic scans of the information system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy;	The organization: a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: - Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or - Inserted through the exploitation of information system vulnerabilities; b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: - Perform periodic scans of the information system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources as the files are

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			- [*Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator;* [*Assignment: organization-defined action*]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Control Enhancements: (1) The organization centrally manages malicious code protection mechanisms. (2) The information system automatically updates malicious code protection mechanisms (including signature definitions). (3) The information system prevents non-privileged users from circumventing malicious code protection capabilities.	and - [*Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator;* [*Assignment: organization-defined action*]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Control Enhancements: (1) The organization centrally manages malicious code protection mechanisms. (2) The information system automatically updates malicious code protection mechanisms (including signature definitions). (3) The information system prevents non-privileged users from circumventing malicious code protection capabilities.	downloaded, opened, or executed in accordance with organizational security policy; and - [*Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator;* [*Assignment: organization-defined action*]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.
EBBD-1 EBVC-1 ECID-1	SI-4	INFORMATION SYSTEM MONITORING	The organization: a. Monitors events on the information system in accordance with [*Assignment: organization-defined monitoring objectives*] and detects information system attacks; b. Identifies unauthorized use of the information system; c. Deploys monitoring devices: (i)	The organization: a. Monitors events on the information system in accordance with [*Assignment: organization-defined monitoring objectives*] and detects information system attacks; b. Identifies unauthorized use of the information system; c. Deploys monitoring devices: (i)	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations. Control Enhancements: (2) The organization employs automated tools to support near real-time analysis of events. (4) The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions. (5) The information system provides near real-time alerts when the following indications of compromise or potential compromise occur: [*Assignment: organization-defined list of compromise*	strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations. Control Enhancements: (2) The organization employs automated tools to support near real-time analysis of events. (4) The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions. (5) The information system provides near real-time alerts when the following indications of compromise or	

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			indicators]. (6) The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.	potential compromise occur: [*Assignment: organization-defined list of compromise indicators*]. (6) The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.	
VIVIM-1	SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	The organization: a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to [*Assignment: organization-defined list of personnel (identified by name and/or by role)*]; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance. Control Enhancement: (1) The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.	The organization: a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to [*Assignment: organization-defined list of personnel (identified by name and/or by role)*]; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	The organization: a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to [*Assignment: organization-defined list of personnel (identified by name and/or by role)*]; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.
DCSS-1	SI-6	SECURITY FUNCTIONALITY	The information system verifies the correct operation of security functions	Not Applicable	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
		VERIFICATION	[*Selection (one or more):* [*Assignment: organization-defined system transitional states*]*; upon command by user with appropriate privilege; periodically every* [*Assignment: organization-defined time-period*]] and [*Selection (one or more): notifies system administrator; shuts the system down; restarts the system;* [*Assignment: organization-defined alternative action(s)*]] when anomalies are discovered.		
ECSD-2	SI-7	SOFTWARE AND INFORMATION INTEGRITY	The information system detects unauthorized changes to software and information. Control Enhancements: (1) The organization reassesses the integrity of software and information by performing [*Assignment: organization-defined frequency*] integrity scans of the information system. (2) The organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification.	The information system detects unauthorized changes to software and information. Control Enhancement: (1) The organization reassesses the integrity of software and information by performing [*Assignment: organization-defined frequency*] integrity scans of the information system.	Not Applicable
---	SI-8	SPAM PROTECTION	The organization: a. Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited	The organization: a. Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and b. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures. Control Enhancement: (1) The organization centrally manages spam protection mechanisms.	messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and b. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.	
---	SI-9	INFORMATION INPUT RESTRICTIONS	The organization restricts the capability to input information to the information system to authorized personnel.	The organization restricts the capability to input information to the information system to authorized personnel.	Not Applicable
---	SI-10	INFORMATION INPUT VALIDATION	The information system checks the validity of information inputs.	The information system checks the validity of information inputs.	Not Applicable
---	SI-11	ERROR HANDLING	The information system: a. Identifies potentially security-relevant error conditions; b. Generates error messages that provide information necessary for corrective actions without revealing [*Assignment: organization-defined sensitive or potentially harmful information*] in error logs and administrative messages that could be exploited by adversaries; and c. Reveals error messages only to authorized personnel.	The information system: a. Identifies potentially security-relevant error conditions; b. Generates error messages that provide information necessary for corrective actions without revealing [*Assignment: organization-defined sensitive or potentially harmful information*] in error logs and administrative messages that could be exploited by adversaries; and c. Reveals error messages only to authorized personnel.	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
PESP-1	SI-12	INFORMATION OUTPUT HANDLING AND RETENTION	The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.
	SI-13	PREDICTABLE FAILURE PREVENTION	Not Applicable	Not Applicable	Not Applicable
Program Management					
	PM-1	INFORMATION SECURITY PROGRAM PLAN	The organization: a. Develops and disseminates an organization-wide information security program plan that: - Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; - Provides sufficient information about the program management controls and common controls (including specification of parameters for any *assignment* and *selection* operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is	The organization: a. Develops and disseminates an organization-wide information security program plan that: - Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; - Provides sufficient information about the program management controls and common controls (including specification of parameters for any *assignment* and *selection* operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is	The organization: a. Develops and disseminates an organization-wide information security program plan that: - Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; - Provides sufficient information about the program management controls and common controls (including specification of parameters for any *assignment* and *selection* operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			implemented as intended; - Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance; - Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Reviews the organization-wide information security program plan [*Assignment: organization-defined frequency*]; and c. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments.	implemented as intended; - Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance; - Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Reviews the organization-wide information security program plan [*Assignment: organization-defined frequency*]; and c. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments.	intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended; - Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance; - Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Reviews the organization-wide information security program plan [*Assignment: organization-defined frequency*]; and c. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments.
	PM-2	SENIOR INFORMATION SECURITY OFFICER	The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.	The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.	The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.
	PM-3	INFORMATION SECURITY RESOURCES	The organization: a. Ensures that all capital planning and investment requests include the	The organization: a. Ensures that all capital planning and investment requests include the	The organization: a. Ensures that all capital planning and investment requests include the

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			resources needed to implement the information security program and documents all exceptions to this requirement; b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and c. Ensures that information security resources are available for expenditure as planned.	resources needed to implement the information security program and documents all exceptions to this requirement; b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and c. Ensures that information security resources are available for expenditure as planned.	resources needed to implement the information security program and documents all exceptions to this requirement; b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and c. Ensures that information security resources are available for expenditure as planned.
	PM-4	PLAN OF ACTION AND MILESTONES PROCESS	The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.	The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.	The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.
	PM-5	INFORMATION SYSTEM INVENTORY	The organization develops and maintains an inventory of its information systems.	The organization develops and maintains an inventory of its information systems.	The organization develops and maintains an inventory of its information systems.
	PM-6	INFORMATION SECURITY MEASURES OF PERFORMANCE	The organization develops, monitors, and reports on the results of information security measures of performance.	The organization develops, monitors, and reports on the results of information security measures of performance.	The organization develops, monitors, and reports on the results of information security measures of performance.
	PM-7	ENTERPRISE ARCHITECTURE	The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the	The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and	The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals,

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			Nation.	the Nation.	other organizations, and the Nation.
	PM-8	CRITICAL INFRASTRUCTURE PLAN	The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.
	PM-9	RISK MANAGEMENT STRATEGY	The organization: a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and b. Implements that strategy consistently across the organization.	The organization: a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and b. Implements that strategy consistently across the organization.	The organization: a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and b. Implements that strategy consistently across the organization.
	PM-10	SECURITY AUTHORIZATION PROCESS	The organization: a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes; b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Fully integrates the security authorization processes into an organization-wide risk management program.	The organization: a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes; b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Fully integrates the security authorization processes into an organization-wide risk management program.	The organization: a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes; b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Fully integrates the security authorization processes into an organization-wide risk management program.
	PM-11	MISSION/ BUSINESS PROCESS DEFINITION	The organization: a. Defines mission/business processes with consideration for information security and the resulting risk to	The organization: a. Defines mission/business processes with consideration for information security and the resulting	The organization: a. Defines mission/business processes with consideration for information security and the

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.

(END OF ATTACHMENT J-3)