ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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.	
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 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	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
			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*].	
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.	
EBBD-1 EBBD-2	AC-4	INFORMATION FLOW ENFORCEMENT	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II))
ECLP-1	AC-5	SEPARATION OF DUTIES	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II))
ECLP-1	AC-6	LEAST PRIVILEGE	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II))

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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 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	Optional: (May be applicable for DoD MAC I or MAC II)
ECLO-1	AC-10	CONCURRENT SESSION CONTROL	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
PESL-1	AC-11	SESSION LOCK	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
---	AC-12	SESSION TERMINATION	Withdrawn: Incorporated into SC-10	Optional: (May be applicable for DoD MAC I or MAC II)
ECAT-1 ECAT-2 E3.3.9	AC-13	SUPERVISION AND REVIEW — ACCESS CONTROL	Withdrawn: Incorporated into AC-2 and AU-6.	Optional: (May be applicable for DoD MAC I or MAC II)
---	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.	
ECML-1	AC-15	AUTOMATED MARKING	Withdrawn: Incorporated into MP-3.	Optional: (May be applicable for DoD MAC I or MAC II)
	AC-16	SECURITY ATTRIBUTES	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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.	
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.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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 accordance with organizational policies and procedures.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
---	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.	
	AC-21	USER-BASED COLLABORATION AND INFORMATION SHARING	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
	AC-22	PUBLICLY ACCESSIBLE CONTENT	The organization: a. Designates individuals authorized to post information onto an organizational information system 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 b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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.	
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.	
---	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*].	
	AT-5	CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
Audit and Accountability				

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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.	
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 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*].	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
ECAR-1 ECAR-2 ECAR-3 ECLC-1	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 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.	
---	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)*].	
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.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
ECRG-1	AU-7	AUDIT REDUCTION AND REPORT GENERATION	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
ECAR-1	AU-8	TIME STAMPS	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.	
	AU-10	NON-REPUDIATION	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
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.	
	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.	
	AU-13	MONITORING FOR INFORMATION DISCLOSURE	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
	AU-14	SESSION AUDIT	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
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.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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 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. .	
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.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
DCAR-1 5.7.5	CA-4	SECURITY CERTIFICATION	Withdrawn: Incorporated into CA-2.	Optional: (May be applicable for DoD MAC I or MAC II)
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 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*].	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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 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.	
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.	
DCPR-1	CM-3	CONFIGURATION CHANGE CONTROL	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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.	
DCPR-1 ECSD-2	CM-5	ACCESS RESTRICTIONS FOR CHANGE	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
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.	
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*].	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
	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.	
	CM-9	CONFIGURATION MANAGEMENT PLAN	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
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.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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 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*]	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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*].	
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.	
DCAR-1	CP-5	CONTINGENCY PLAN UPDATE	Withdrawn: Incorporated into CP-2.	May be applicable for DoD MAC I or MAC II)
CODB-2	CP-6	ALTERNATE STORAGE SITE	Not Applicable	May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
COAS-1 COEB-1 COSP-1 COSP-2	CP-7	ALTERNATE PROCESSING SITE	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
---	CP-8	TELECOMMUNICA-TIONS SERVICES	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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 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 RECONSTITUTION	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	
Identification and Authentication				

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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 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 Enhancement: (1) The information system uses multifactor authentication for network access to privileged accounts.	
---	IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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*].	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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 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 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*	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
---	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.	
---	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.	
	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).	
Incident Response				
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.	
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*].	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
VIIR-1	IR-3	INCIDENT RESPONSE TESTING AND EXERCISES	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
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.	
VIIR-1	IR-5	INCIDENT MONITORING	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.	
---	IR-7	INCIDENT RESPONSE ASSISTANCE	The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
	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 - 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*].	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
		Maintenance		
PRMP-1 DCAR-1	MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) 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 following maintenance or repair actions.	
---	MA-3	MAINTENANCE TOOLS	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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; d. Maintains records for non-local maintenance and diagnostic activities; and e. Terminates all sessions and network connections when non-local maintenance is completed.	
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.	
COMS-1 COSP-1	MA-6	TIMELY MAINTENANCE	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
Media Protection				

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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.	
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].	
ECML-1	MP-3	MEDIA MARKING	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
PESS-1	MP-4	MEDIA STORAGE	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
---	MP-5	MEDIA TRANSPORT	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
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.	
PEDD-1	MP-7	MEDIA DESTRUCTION AND DISPOSAL	Withdrawn from SP 800-53, Rev. 3	Optional: (May be applicable for DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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.	
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.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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 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	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
PEDI-1 PEPF-1	PE-5	ACCESS CONTROL FOR OUTPUT DEVICES	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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 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.	
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 [*Assignment: organization-defined frequency*].	
---	PE-9	POWER EQUIPMENT AND POWER CABLING	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
PEMS-1	PE-10	EMERGENCY SHUTOFF	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
COPS-1 COPS-2 COPS-3	PE-11	EMERGENCY POWER	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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.	
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.	
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*].	
---	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.	
---	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.	
EBRU-1	PE-17	ALTERNATE WORK SITE	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
	PE-18	LOCATION OF INFORMATION SYSTEM COMPONENTS	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
	PE-19	INFORMATION LEAKAGE	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
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.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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 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.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
5.7.5	PL-3	SYSTEM SECURITY PLAN UPDATE	Withdrawn: Incorporated into PL-2.	Optional: (May be applicable for DoD MAC I or MAC II)
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.	
---	PL-5	PRIVACY IMPACT ASSESSMENT	The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.	
	PL-6	SECURITY-RELATED ACTIVITY PLANNING	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
Personnel Security				

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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.	
---	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*].	
PRAS-1	PS-3	PERSONNEL SCREENING	The organization: a. Screens individuals prior to authorizing access to the information system; and 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*].	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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.	
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*].	
PRRB-1	PS-6	ACCESS AGREEMENTS	The organization: a. Ensures that individuals requiring 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.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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.	
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 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.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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 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.	Optional: (May be applicable for DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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 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).	
System and Services Acquisition				

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
DCAR-1	SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: 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.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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 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.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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: - 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.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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.	
---	SA-7	USER INSTALLED SOFTWARE	The organization enforces explicit rules governing the installation of software by users.	
DCBP-1 DCCS-1 E3.4.4	SA-8	SECURITY DESIGN PRINCIPLES	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
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.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
---	SA-10	DEVELOPER CONFIGURATION MANAGEMENT	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
E3.4.4	SA-11	DEVELOPER SECURITY TESTING	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
	SA-12	SUPPLY CHAIN PROTECTION	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
	SA-13	TRUSTWORTHI-NESS	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
	SA-14	CRITICAL INFORMATION SYSTEM COMPONENTS	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
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.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
DCPA-1	SC-2	APPLICATION PARTITIONING	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
DCSP-1	SC-3	SECURITY FUNCTION ISOLATION	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
ECRC-1	SC-4	INFORMATION IN SHARED RESOURCES	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
---	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*].	
---	SC-6	RESOURCE PRIORITY	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
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.	
ECTM-1	SC-8	TRANSMISSION INTEGRITY	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
ECCT-1	SC-9	TRANSMISSION CONFIDENTIALITY	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
---	SC-10	NETWORK DISCONNECT	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
	SC-11	TRUSTED PATH	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
IAKM-1	SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	The organization establishes and manages cryptographic keys for required cryptography employed within the information system.	
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.	
EBPW-1	SC-14	PUBLIC ACCESS PROTECTIONS	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.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
	SC-16	TRANSMISSION OF SECURITY ATTRIBUTES	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
IAKM-1	SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
DCMC-1	SC-18	MOBILE CODE	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
ECVI-1	SC-19	VOICE OVER INTERNET PROTOCOL	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
	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 supports secure resolution services) enable verification of a chain of trust among parent and child domains.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
	SC-21	SECURE NAME / ADDRESS RESOLUTION SERVICE (Recursive or Caching Resolver)	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
	SC-22	ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
	SC-23	SESSION AUTHENTICITY	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
	SC-24	FAIL IN KNOWN STATE	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
	SC-25	THIN NODES	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
	SC-26	HONEYPOTS	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
	SC-27	OPERATING SYSTEM-INDEPENDENT APPLICATIONS	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
	SC-28	PROTECTION OF INFORMATION AT REST	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
	SC-29	HETEROGENEITY	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
	SC-30	VIRTUALIZATION TECHNIQUES	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
	SC-31	COVERT CHANNEL ANALYSIS	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
	SC-32	INFORMATION SYSTEM PARTITIONING	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
	SC-33	TRANSMISSION PREPARATION INTEGRITY	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
	SC-34	NON-MODIFIABLE EXECUTABLE PROGRAMS	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
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.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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 - [*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	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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.	
DCSS-1	SI-6	SECURITY FUNCTIONALITY VERIFICATION	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
ECSD-2	SI-7	SOFTWARE AND INFORMATION INTEGRITY	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
---	SI-8	SPAM PROTECTION	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
---	SI-9	INFORMATION INPUT RESTRICTIONS	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
---	SI-10	INFORMATION INPUT VALIDATION	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
---	SI-11	ERROR HANDLING	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
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.	
	SI-13	PREDICTABLE FAILURE PREVENTION	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
Program Management				

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
	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 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.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
	PM-3	INFORMATION SECURITY RESOURCES	The organization: a. Ensures that all capital planning and investment requests include the 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.	
	PM-5	INFORMATION SYSTEM INVENTORY	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.	
	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 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.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
	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.	
	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.	
	PM-11	MISSION/ BUSINESS PROCESS DEFINITION	The organization: a. Defines mission/business processes with consideration for information security and the 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-2)