



**Department of Veterans Affairs  
Office of IT Oversight and**

**Facility Assessment**

**Version 1.0**

**March 2007**

***For Department of Veterans Affairs Limited  
Official Use Only***

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
AC-1 Access Control Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.	The access control policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.	None	
AC-2 Account Management	The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [Assignment: organization-defined frequency, at least annually].	Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on: (i) a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. Account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' information system usage or need-to-know/need-to-share changes.	(1) The organization employs automated mechanisms to support the management of information system accounts. (2) The information system automatically terminates temporary and emergency accounts after [Assignment: organization-defined time period for each type of account]. (3) The information system automatically disables inactive accounts after [Assignment: organization-defined time period]. (4) The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
AC-3 Access Enforcement	The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.	Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended)	(1) The information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel. Enhancement Supplemental Guidance: Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users. Privileged users are individuals who have access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).	
Information Flow Enforcement	The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few, of many, generalized examples of possible restrictions that are better expressed as flow control than access control are: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, firewalls, intrusion detection systems, etc.)	(1) The information system implements information flow control enforcement using explicit labels on information, source, and destination objects as a basis for flow control decisions. Enhancement Supplemental Guidance: Information flow control enforcement using explicit labels is used, for example, to control the release of certain types of information. (2) The information system implements information flow control enforcement using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decisions. (3) The information system implements information flow control enforcement using dynamic security policy mechanisms as a basis for flow control decisions.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
Separation of Duties	The information system enforces separation of duties through assigned access authorizations.	The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.	None	
Least Privilege	The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.	The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals.	None	
AC-7 Unsuccessful Login Attempts	The information system enforces a limit of [Assignment: organization-defined number] consecutive invalid access attempts by a user during a [Assignment: organization-defined time period] time period. The information system automatically [Selection: locks the account/node for an [Assignment: organization-defined time period], delays next login prompt according to Assignment: organization-defined delay algorithm.]] when the maximum number of unsuccessful attempts is exceeded.	Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization.	(1) The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
AC-8 System Use Notification	The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.	Privacy and security policies are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems: (i) the system use information is available and when appropriate, is displayed before granting access; (ii) any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and (iii) the notice given to public users of the information system includes a description of the authorized uses of the system.	None	
Previous Login Notification	The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.	None	None	
Concurrent Session Control	The information system limits the number of concurrent sessions for any user to [Assignment: organization-defined number of sessions].	None	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
Session Lock	The information system prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.	Users can directly initiate session lock mechanisms. A session lock is not a substitute for logging out of the information system. Organization-defined time periods of inactivity comply with federal policy; for example, in accordance with OMB Memorandum 06-16, the organization-defined time period is no greater than thirty minutes for remote access and portable devices.	None	
Session Termination	The information system automatically terminates a remote session after [Assignment: organization-defined time period] of inactivity.	A remote session is initiated whenever an organizational information system is accessed by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).	(1) Automatic session termination applies to local and remote sessions.	
AC-13 Supervision and Review--Access Control	The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.	The organization reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization investigates any unusual information system-related activities and periodically reviews changes to access authorizations. The organization reviews more frequently the activities of users with significant information system roles and responsibilities. The extent of the audit record reviews is based on the FIPS 199 impact level of the information system. For example, for low-impact systems, it is not intended that security logs be reviewed frequently for every workstation, but rather at central points such as a web proxy or email servers and when specific circumstances warrant review of other audit records. NIST Special Publication 800-92 provides guidance on computer security log management.	(1) The organization employs automated mechanisms to facilitate the review of user activities.	
AC-14 Permitted Actions Without Identification and Authentication	The organization identifies and documents specific user actions that can be performed on the information system without identification or authentication.	The organization allows limited user activity without identification and authentication for public websites or other publicly available information systems (e.g., individuals accessing a federal information system at <a href="http://www.firstgov.gov">http://www.firstgov.gov</a> ). Related security control: IA-2.	(1) The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.	
Automated Marking	The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.	Automated marking refers to markings employed on external media (e.g., hardcopy documents output from the information system). The markings used in external marking are distinguished from the labels used on internal data structures described in AC-16.	None	
Automated Labeling	The information system appropriately labels information in storage, in process, and in transmission.	Automated labeling refers to labels employed on internal data structures (e.g., records, files) within the information system. Information labeling is accomplished in accordance with: (i) access control requirements; (ii) special dissemination, handling, or distribution instructions; or (iii) as otherwise required to enforce information system security policy.	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
AC-17 Remote Access	The organization authorizes, monitors, and controls all methods of remote access to the information system.	Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). NIST Special Publication 800-63 provides guidance on remote electronic authentication. If the federal Personal Identity Verification (PIV) credential is used as an identification token where cryptographic token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST Special Publications 800-73 and 800-78. NIST Special Publication 800-77 provides	(1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods. (2) The organization uses cryptography to protect the confidentiality and integrity of remote access sessions. (3) The organization controls all remote accesses through a limited number of managed access control points. (4) The organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system.	
AC-18 Wireless Access Restrictions	The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) authorizes, monitors, controls wireless access to the information system.	NIST Special Publications 800-48 and 800-97 provide guidance on wireless network security. NIST Special Publication 800-94 provides guidance on wireless intrusion detection and prevention.	(1) The organization uses authentication and encryption to protect wireless access to the information system. (2) The organization scans for unauthorized wireless	
Access Control for Portable and Mobile Devices	The organization: (i) establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and (ii) authorizes, monitors, and controls device access to organizational information systems.	Portable and mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are only allowed access to organizational information systems in accordance with organizational security policies and procedures. Security policies and procedures include device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), configuration management, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Protecting information residing on portable and mobile devices (e.g., employing cryptographic mechanisms to provide confidentiality and integrity protections during storage and while in transit when outside of controlled area	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
AC-20 Use of External Information Systems	The organization establishes terms and conditions for authorized individuals to: (i) access the information system from an external information system; and (ii) process, store, and/or transmit organization-controlled information using an external information system.	External information systems are information systems or components of information systems that are outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to, personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); information systems owned or controlled by nonfederal governmental organizations; and federal information systems that are not owned by, operated by, or under the direct control of the organization.  Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system. This control does not apply to the use of external information systems to access organizational information systems and	(1) The organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization: (i) can verify the employment of required security controls on the external system as specified in the organization's information security policy and system security plan; or (ii) has approved information system connection or processing agreements with the organizational entity hosting the external information system.	
AT-1 Security Awareness and Training Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	The security awareness and training policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publications 800-16 and 800-50 provide guidance on security awareness and training. NIST Special Publication 800-12 provides guidance on security policies and procedures.	None	
AT-2 Security Awareness	The organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and [Assignment: organization-defined frequency, at least annually] thereafter.	The organization determines the appropriate content of security awareness training based on the specific requirements of the organization and the information systems to which personnel have authorized access. The organization's security awareness program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST Special Publication 800-50.	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
AT-3 Security Training	The organization identifies personnel that have significant information system security roles and responsibilities during the system development life cycle, documents those roles and responsibilities, and provides appropriate information system security training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [Assignment: organization-defined frequency] thereafter.	The organization determines the appropriate content of security training based on the specific requirements of the organization and the information systems to which personnel have authorized access. In addition, the organization provides system managers, system and network administrators, and other personnel having access to system-level software, adequate technical training to perform their assigned duties. The organization's security training program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST Special Publication 800-50.	None	
AT-4 Security Training Records	The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.	None	None	
Contacts with Security Groups and Associations	The organization establishes and maintains contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations to stay up to date with the latest recommended security practices, techniques, and technologies and to share the latest security-related information including threats, vulnerabilities, and incidents.	To facilitate ongoing security education and training for organizational personnel in an environment of rapid technology changes and dynamic threats, the organization establishes and institutionalizes contacts with selected groups and associations within the security community. The groups and associations selected are in keeping with the organization's mission requirements. Information sharing activities regarding threats, vulnerabilities, and incidents related to information systems are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.	None	
AU-1 Audit and Accountability Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	The audit and accountability policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
AU-2 Auditable Events	The information system generates audit records for the following events: [Assignment: organization-defined auditable events].	The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverse the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The checklists and configuration guides at <a href="http://csrc.nist.gov/pcig/cig.html">http://csrc.nist.gov/pcig/cig.html</a> pr	(1) The information system provides the capability to compile audit records from multiple components throughout the system wide (logical or physical), time-correlated audit trail. (2) The information system provides the capability to manage the selection of events to be audited by individual components of the system. (3) The organization periodically reviews and updates the list of organization-defined auditable events.	
AU-3 Content of Audit Records	The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.	Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (success or failure) of the event. NIST Special Publication 800-92 provides guidance on computer security log management.	(1) The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject. (2) The information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.	
AU-4 Audit Storage Capacity	The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	The organization provides sufficient audit storage capacity, taking into account the auditing to be performed and the online audit processing requirements. Related security controls: AU-2, AU-5, AU-6, AU-7, SI-4.	None	
AU-5	The information system alerts appropriate organizational officials in the event of an audit processing failure and 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)].	Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Related security control: AU-4.	(1) The information system provides a warning when allocated audit record storage volume reaches [Assignment: organization-defined percentage of maximum audit record storage capacity]. (2) The information system provides a real-time alert when the following audit failure events occur: [Assignment: organization-defined audit failure events requiring real-time alerts].	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
Audit Monitoring, Analysis, and Reporting	The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.	Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.	(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities. (2) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts].	
Audit Reduction and Report Generation	The information system provides an audit reduction and report generation capability.	Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents without altering original audit records.	(1) The information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.	
AU-8 Time Stamps	The information system provides time stamps for use in audit record generation.	Time stamps (including date and time) of audit records are generated using internal system clocks.	(1) The organization synchronizes internal information system clocks [Assignment: organization-defined frequency].	
AU-9 Protection of Audit Information	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.	(1) The information system produces audit records on hardware-enforced, write-once media.	
Non-Repudiation	The information system provides the capability to determine whether a given individual took a particular action.	Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message. Non-repudiation protects against later false claims by an individual of not having taken a specific action. Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts, time stamps).	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
AU-11 Audit Record Retention	The organization retains audit records for [Assignment: organization-defined time period] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	The organization retains audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions. Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. NIST Special Publication 800-61 provides guidance on computer security incident handling and audit record retention.	None	
CA-1 Certification, Accreditation, and Security Assessment Policies and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.	The security assessment and certification and accreditation policies and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security assessment and certification and accreditation policies can be included as part of the general information security policy for the organization. Security assessment and certification and accreditation procedures can be developed for the security program in general, and for a particular information system, when required. The organization defines what constitutes a significant change to the information system to achieve consistent security reaccreditations. NIST Special Publication 800-53A provides guidance on security control assessments. NIST Special Publication 800-37 provides guidance on security certification and accreditation. NIST Special Publication 800-12 provides guidance on security policies and procedures.	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
CA-2 Security Assessments	The organization conducts an assessment of the security controls in the information system [Assignment: organization-defined frequency, at least annually] 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.	This control is intended to support the FISMA requirement that the management, operational, and technical controls in each information system contained in the inventory of major information systems be assessed with a frequency depending on risk, but no less than annually. The FISMA requirement for (at least) annual security control assessments should not be interpreted by organizations as adding additional assessment requirements to those requirements already in place in the security certification and accreditation process. To satisfy the annual FISMA assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to: (i) security certifications conducted as part of an information system accreditation or reaccreditation process (see CA-4); (ii) continuous monitoring activities (see CA-7); or (iii) testing and evaluation of the information system as part of the ongoing system development life cycle process (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). OMB does not require an annual assessment of all security controls.	None	
CA-3 Information System Connections	The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.	Since FIPS 199 security categorizations apply to individual information systems, the organization carefully considers the risks that may be introduced when systems are connected to other information systems with different security requirements and security controls, both within the organization and external to the organization. Risk considerations also include information systems sharing the same networks. NIST Special Publication 800-47 provides guidance on connecting information systems. Related security controls: SC-7, SA-9.	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
CA-4 Security Certification	The organization conducts an assessment of the security controls in the information system 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.	A security certification is conducted by the organization in support of the OMB Circular A-130, Appendix III requirement for accrediting the information system. The security certification is a key factor in all security accreditation (i.e., authorization) decisions and is integrated into and spans the system development life cycle. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring (see CA-7). The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-2). NIST Special Publication 800-53A provides guidance on security control assessments. NIST Special Publication 800-37 provides guidance on security certification and accreditation. Related security controls: CA-2, CA-6, SA-11.	(1) The organization employs an independent certification agent or certification team to conduct an assessment of the security controls in the information system. Enhancement Supplemental Guidance: An independent certification agent or certification team is any individual or group capable of conducting an impartial assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain of command associated with the information system or to the determination of security control effectiveness. Independent security certification services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted certification services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the independence of the certification agent or certification team conducting the assessment of the	
CA-5 Plan of Action and Milestones	The organization develops and updates [Assignment: organization-defined frequency], a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.	The plan of action and milestones is a key document in the security accreditation package developed for the authorizing official and is subject to federal reporting requirements established by OMB. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones. NIST Special Publication 800-37 provides guidance on the security certification and accreditation of information systems. NIST Special Publication 800-30 provides guidance on risk mitigation.	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
CA-6 Security Accreditation	The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization [Assignment: organization-defined frequency, at least every three years] or when there is a significant change to the system. A senior organizational official signs and approves the security accreditation.	OMB Circular A-130, Appendix III, establishes policy for security accreditations of federal information systems. The organization assesses the security controls employed within the information system before and in support of the security accreditation. Security assessments conducted in support of security accreditations are called security certifications. The security accreditation of an information system is not a static process. Through the employment of a comprehensive continuous monitoring process (the fourth and final phase of the certification and accreditation process), the critical information contained in the accreditation package (i.e., the system security plan, the security assessment report, and the plan of action and milestones) is updated on an ongoing basis providing the authorizing official and the information system owner with an up-to-date status of the security state of the information system. To reduce the administrative burden of the three-year reaccreditation process, the authorizing official uses the results of the ongoing continuous monitoring process to the maximum extent possible.	None	
CA-7 Continuous Monitoring	The organization monitors the security controls in the information system on an ongoing basis.	Continuous monitoring activities include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring. The selection of an appropriate subset of security controls is based on: (i) the FIPS 199 security categorization of the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; and (iii) the level of assurance (or grounds for confidence) that the organization must have in determining the effectiveness of the security controls in the information system. The organization establishes the selection criteria and subsequently selects a subset of the security controls employed within the information system. This control is closely related to and mutually supportive of CA-6.	(1) The organization employs an independent certification agent or certification team to monitor the security controls in the information system on an ongoing basis. Enhancement Supplemental Guidance: The organization can extend and maximize the value of the ongoing assessment of security controls during the continuous monitoring process by requiring an independent certification agent or team to assess all of the security controls during the information system's three-year accreditation cycle. Related security controls: CA-2, CA-4, CA-5, CA-6, CM-4.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
CM-1 Configuration Management Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	The configuration management policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.	None	
CM-2 Baseline Configuration	The organization develops, documents, and maintains a current baseline configuration of the information system.	This control establishes a baseline configuration for the information system. The baseline configuration provides information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the information system architecture. The baseline configuration also provides the organization with a well-defined and documented specification to which the information system is built and deviations, if required, are documented in support of mission needs/objectives. The baseline configuration of the information system is consistent with the Federal Enterprise Architecture. Related security controls: CM-6, CM-8.	(1) The organization updates the baseline configuration of the information system as an integral part of information system component installations. (2) The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.	
Configuration Change Control	The organization authorizes, documents, and controls changes to the information system.	The organization manages configuration changes to the information system using an organizationally approved process (e.g., a chartered Configuration Control Board). Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications. Configuration change control includes changes to the configuration settings for information technology products (e.g., operating systems, firewalls, routers). The organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws. The approvals to implement a change to the information system include successful results from the security analysis of the change. The organization audits activities associated with configuration changes to the information system. Related security controls: CM-4, CM-6, SI-2	(1) The organization employs automated mechanisms to: (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
Monitoring Configuration Changes	The organization monitors changes to the information system conducting security impact analyses to determine the effects of the changes.	Prior to change implementation, and as part of the change approval process, the organization analyzes changes to the information system for potential security impacts. After the information system is changed (including upgrades and modifications), the organization checks the security features to verify that the features are still functioning properly. The organization audits activities associated with configuration changes to the information system. Monitoring configuration changes and conducting security impact analyses are important elements with regard to the ongoing assessment of security controls in the information system. Related security control: CA-7.	None	
Access Restrictions for Change	The organization: (i) approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and (ii) generates, retains, and reviews records reflecting all such changes.	Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals obtain access to information system components for purposes of initiating changes, including upgrades, and modifications.	(1) The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.	
CM-6 Configuration Settings	The organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system.	Configuration settings are the configurable parameters of the information technology products that compose the information system. Organizations monitor and control changes to the configuration settings in accordance with organizational policies and procedures. OMB FISMA reporting instructions provide guidance on configuration requirements for federal information systems. NIST Special Publication 800-70 provides guidance on producing and using configuration settings for information technology products employed in organizational information systems. Related security controls: CM-2, CM-3, SI-4.	(1) The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
Least Functionality	The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined list of prohibited and/or restricted functions, ports, protocols, and/or services].	Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of an information system, but doing so increases risk over limiting the services provided by any one component. Where feasible, the organization limits component functionality to a single function per device (e.g., email server or web server, not both). The functions and services provided by information systems, or individual components of information systems, are carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, file sharing).	(1) The organization reviews the information system [Assignment: organization-defined frequency], to identify and eliminate unnecessary functions, ports, protocols, and/or services.	
CM-8 Information System Component Inventory	The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information.	The organization determines the appropriate level of granularity for the information system components included in the inventory that are subject to management control (i.e., tracking, and reporting). The inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner). The component inventory is consistent with the accreditation boundary of the information system. Related security controls: CM-2, CM-6.	(1) The organization updates the inventory of information system components as an integral part of component installations. (2) The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.	
CP-1 Contingency Planning Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	The contingency planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-34 provides guidance on contingency planning. NIST Special Publication 800-12 provides guidance on security policies and procedures.	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
CP-2 Contingency Plan	The organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.	None	(1) The organization coordinates contingency plan development with organizational elements responsible for related plans. Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan. (2) The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations.	
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, at least annually].	None	(1) The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations. (2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.	
Contingency Plan Testing and Exercises	The organization: (i) tests and/or exercises the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and/or exercises] to determine the plan's effectiveness and the organization's readiness to execute the plan; and (ii) reviews the contingency plan test/exercise results and initiates corrective actions.	There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., full-scale contingency plan testing, functional/tabletop exercises). The depth and rigor of contingency plan testing and/or exercises increases with the FIPS 199 impact level of the information system. Contingency plan testing and/or exercises also include a determination of the effects on organizational operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan. NIST Special Publication 800-84 provides guidance on test, training, and exercise programs for information technology plans and capabilities.	(1) The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans. Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan. (2) The organization tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations. (3) The organization employs automated mechanisms to more thoroughly and effectively test/exercise the contingency plan by providing more complete coverage of contingency issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the information system and supported missions.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
CP-5 Contingency Plan Update	The organization reviews the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.	Organizational changes include changes in mission, functions, or business processes supported by the information system. The organization communicates changes to appropriate organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, Emergency Action Plan).	None	
Alternate Storage Site	The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.	The frequency of information system backups and the transfer rate of backup information to the alternate storage site (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives.	(1) The organization identifies an alternate storage site that is geographically separated from the primary storage site so as not to be susceptible to the same hazards. (2) The organization configures the alternate storage site to facilitate timely and effective recovery operations. (3) The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	
Alternate Processing Site	The organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within [Assignment: organization-defined time period] when the primary processing capabilities are unavailable.	Equipment and supplies required to resume operations within the organization-defined time period are either available at the alternate site or contracts are in place to support delivery to the site. Timeframes to resume information system operations are consistent with organization-established recovery time objectives.	(1) The organization identifies an alternate processing site that is geographically separated from the primary processing site so as not to be susceptible to the same hazards. (2) The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions. (3) The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements. (4) The organization fully configures the alternate processing site so that it is ready to be used as the operational site supporting a minimum required operational capability.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
Telecommunications Services	The organization identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable.	In the event that the primary and/or alternate telecommunications services are provided by a common carrier, the organization requests Telecommunications Service Priority (TSP) for all telecommunications services used for national security emergency preparedness (see <a href="http://tsp.ncs.gov">http://tsp.ncs.gov</a> for a full explanation of the TSP program).	<p>(1) The organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.</p> <p>(2) The organization obtains alternate telecommunications services that do not share a single point of failure with primary telecommunications services.</p> <p>(3) The organization obtains alternate telecommunications service providers that are sufficiently separated from primary service providers so as not to be susceptible to the same hazards.</p> <p>(4) The organization requires primary and alternate telecommunications service providers to have adequate contingency plans.</p>	
CP-9 Information System Backup	The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [Assignment: organization-defined frequency] and protects backup information at the storage location.	The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives. While integrity and availability are the primary concerns for system backup information, protecting backup information from unauthorized disclosure is also an important consideration depending on the type of information residing on the backup media and the FIPS 199 impact level. An organizational assessment of risk guides the use of encryption for backup information. The protection of system backup information while in transit is beyond the scope of this control. Related security controls: MP-4, MP-5.	<p>(1) The organization tests backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.</p> <p>(2) The organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing.</p> <p>(3) The organization stores backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.</p> <p>(4) The organization protects system backup information from unauthorized modification. Enhancement Supplemental Guidance: The organization employs appropriate mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of information system backups. Protecting the confidentiality of system backup information is beyond the scope of this control. Related security controls: MP-4, MP-5.</p>	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
CP-10 Information System Recovery and Reconstitution	The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.	Information system recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested.	(1) The organization includes a full recovery and reconstitution of the information system as part of contingency plan testing.	
IA-1 Identification and Authentication Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	The identification and authentication policy and procedures are consistent with: (i) FIPS 201 and Special Publications 800-73, 800-76, and 800-78; and (ii) other applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. NIST Special Publication 800-63 provides guidance on remote electronic authentication.	None	
IA-2 User Identification and Authentication	The information system uniquely identifies and authenticates users (or processes acting on behalf of users).	Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance security control AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. NIST Special Publication 800-63 provides guidance on remote electronic authentication including strength of authentication mechanisms. For purposes of this control, the guidance provided in Special Publication 800-63 is applied to both local and remote access to information systems. Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Local access is any access to an organizational information system by a user (or an information system) communicating through an internal organization-controlled network (e.g., local area network) or directly to a device without the use of a network. Unless a more stringent policy is established, the organization shall implement multifactor authentication for remote system access that is NIST Special Publication 800-63 level 3 or level 4 compliant. In accordance with OMB policy and E-Authentication E-G...	(1) The information system employs multifactor authentication for remote system access that is NIST Special Publication 800-63 [Selection: organization-defined level 3, level 3 using a hardware authentication device, or level 4] compliant. (2) The information system employs multifactor authentication for local system access that is NIST Special Publication 800-63 [Selection: organization-defined level 3 or level 4] compliant. (3) The information system employs multifactor authentication for remote system access that is NIST Special Publication 800-63 level 4 compliant.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
Device Identification and Authentication	The information system identifies and authenticates specific devices before establishing a connection.	The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Protocol/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the FIPS 199 security categorization of the information system with higher impact levels requiring stronger authentication.	None	
IA-4 Identifier Management	The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) issuing the user identifier to the intended party; (v) disabling the user identifier after [Assignment: organization-defined time period] of inactivity; and (vi) archiving user identifiers.	Identifier management is not applicable to shared information system accounts (e.g., guest and anonymous accounts). FIPS 201 and Special Publications 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors.	None	
IA-5 Authenticator Management	The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.	Information system authenticators include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. For password-based authentication, the information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations. For PKI-based authentication, the information system: (i) validates certificates by constructing a certification path to an accepted trust anchor; (ii) establishes user control of the corresponding private key; and (iii) maps the authenticated identity to the user account. In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal informati	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
IA-6 Authenticator Feedback	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password is an example of obscuring feedback of authentication information.	None	
IA-7 Cryptographic Module Authentication	The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.	The applicable federal standard for authentication to a cryptographic module is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect, and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. Additional information on the use of validated cryptography is available at <a href="http://csrc.nist.gov/cryptval">http://csrc.nist.gov/cryptval</a> .	None	
IR-1 Incident Response and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.	The incident response policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. NIST Special Publication 800-61 provides guidance on incident handling and reporting. NIST Special Publication 800-83 provides guidance on malware incident handling and prevention.	None	
Incident Response Training	The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training [Assignment: organization-defined frequency, at least annually].	None	(1) The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations. (2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.	
Incident Response Testing and Exercises	The organization tests and/or exercises the incident response capability for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and/or exercises] to determine the incident response effectiveness and documents the results.	NIST Special Publication 800-84 provides guidance on test, training, and exercise programs for information technology plans and capabilities.	(1) The organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability. Enhancement Supplemental Guidance: Automated mechanisms can provide the ability to more thoroughly and effectively test or exercise the capability by providing more complete coverage of incident response issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the response capability.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
IR-4 Incident Handling	The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.	Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The organization incorporates the lessons learned from ongoing incident handling activities into the incident response procedures and implements the procedures accordingly. Related security controls: AU-6, PE-6.	(1) The organization employs automated mechanisms to support the incident handling process.	
Incident Monitoring	The organization tracks and documents information system security incidents on an ongoing basis.	None	(1) The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.	
IR-6 Incident Reporting	The organization promptly reports incident information to appropriate authorities.	The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Organizational officials report cyber security incidents to the United States Computer Emergency Readiness Team (US-CERT) at <a href="http://www.us-cert.gov">http://www.us-cert.gov</a> within the specified timeframe designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. In addition to incident information, weaknesses and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents. NIST Special Publication 800-61 provides guidance on incident reporting.	(1) The organization employs automated mechanisms to assist in the reporting of security incidents.	
IR-7 Incident Response Assistance	The organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability.	Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required.	(1) The organization employs automated mechanisms to increase the availability of incident response-related information and support.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
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, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	The information system maintenance policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.	None	
MA-2 Controlled Maintenance	The organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.	All maintenance activities to include routine, scheduled maintenance and repairs are controlled; whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. Organizational officials approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, the organization removes all information from associated media using approved procedures. After maintenance is performed on the information system, the organization checks all potentially impacted security controls to verify that the controls are still functioning properly.	(1) The organization maintains maintenance records for the information system that include: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable). (2) The organization employs automated mechanisms to schedule and conduct maintenance as required, and to create up-to date, accurate, complete, and available records of all maintenance actions, both needed and completed.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
Maintenance Tools	The organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.	The intent of this control is to address hardware and software brought into the information system specifically for diagnostic/repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and/or software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this control.	<p>(1) The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications. Enhancement Supplemental Guidance: Maintenance tools include, for example, diagnostic and test equipment used to conduct maintenance on the information system.</p> <p>(2) The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.</p> <p>(3) The organization checks all maintenance equipment with the capability of retaining information so that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate organization official explicitly authorizes an exception.</p> <p>(4) The organization employs automated mechanisms</p>	
MA-4 Remote Maintenance	The organization authorizes, monitors, and controls any remotely executed maintenance and diagnostic activities, if employed.	Remote maintenance and diagnostic activities are conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet). The use of remote maintenance and diagnostic tools is consistent with organizational policy and documented in the security plan for the information system. The organization maintains records for all remote maintenance and diagnostic activities. Other techniques and/or controls to consider for improving the security of remote maintenance include: (i) encryption and decryption of communications; (ii) strong identification and authentication techniques, such as Level 3 or 4 tokens as described in NIST Special Publication 800-63; and (iii) remote disconnect verification. When remote maintenance is completed, the organization (or information system in certain cases) terminates all sessions and remote connections invoked in the performance of that activity. If password-based authentication is used to accomplish remote maintenance, the organization changes the passwords following each remote maintenance service. NIST Special	<p>(1) The organization audits all remote maintenance and diagnostic sessions and appropriate organizational personnel review the maintenance records of the remote sessions.</p> <p>(2) The organization addresses the installation and use of remote maintenance and diagnostic links in the security plan for the information system.</p> <p>(3) The organization does not allow remote maintenance or diagnostic services to be performed by a provider that does not implement for its own information system, a level of security at least as high as that implemented on the system being serviced, unless the component being serviced is removed from the information system and sanitized (with regard to organizational information) before the service begins and also sanitized (with regard to potentially malicious software) after the service is performed and before being reconnected to the information system.</p>	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
MA-5 Maintenance Personnel	The organization allows only authorized personnel to perform maintenance on the information system.	Maintenance personnel (whether performing maintenance locally or remotely) have appropriate access authorizations to the information system when maintenance activities allow access to organizational information or could result in a future compromise of confidentiality, integrity, or availability. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the information system.	None	
Timely Maintenance	The organization obtains maintenance support and spare parts for [Assignment: organization-defined list of key information system components] within [Assignment: organization-defined time period] of failure.	None	None	
MP-1 Media Protection Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.	The media protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The media protection policy can be included as part of the general information security policy for the organization. Media protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
MP-2 Media Access	The organization restricts access to information system media to authorized individuals.	Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or i	(1) The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted. Enhancement Supplemental Guidance: This control enhancement is primarily applicable to designated media storage areas within an organization where a significant volume of media is stored and is not intended to apply to every location where some media is stored (e.g., in individual offices).	
Media Labeling	The organization: (i) affixes external labels to removable information system media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information; and (ii) exempts [Assignment: organization-defined list of media types or hardware components] from labeling so long as they remain within [Assignment: organization-defined protected environment].	An organizational assessment of risk guides the selection of media requiring labeling. Organizations document in policy and procedures, the media requiring labeling and the specific measures taken to afford such protection. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, labeling is not required for media containing information determined by the organization to be in the public domain or to be publicly releasable.	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
Media Storage	The organization physically controls and securely stores information system media within controlled areas.	<p>Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. This control applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel exercise extreme caution in the types of information stored on telephone voicemail systems.</p> <p>An organizational assessment of risk guides the selection of information system media. As part of a defense-in-depth protection strategy, the organization</p>	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
Media Transport	The organization protects and controls information system media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel.	Information system media includes both digital media (e.g., diskettes, tapes, removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. This control also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones) that are transported outside of controlled areas. Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel exercise extreme caution in the types of information stored on tele	<p>(1) The organization protects digital and non-digital media during transport outside of controlled areas using [Assignment: organization-defined security measures, e.g., locked container, cryptography]. Enhancement Supplemental Guidance: Physical and technical security measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FIPS 199 security categorization of the information residing on the media, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cryptographic mechanisms can provide confidentiality and/or integrity protections depending upon the mechanisms used.</p> <p>(2) The organization documents, where appropriate, activities associated with the transport of information system media using [Assignment: organization-defined system of records]. Enhancement Supplemental Guidance: Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk.</p> <p>(3) The organization employs an identified custodian at Enhancement Supplemental Guidance: Organization</p>	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
MP-6 Media Sanitization and Disposal	The organization sanitizes information system media, both digital and non-digital, prior to disposal or release for reuse.	Sanitization is the process used to remove information from information system media such that there is reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of organizational information to unauthorized individuals when such media is reused or disposed. The organization uses its discretion on sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on the organization or individuals if released for reuse or disposed. NIST Special Publication 800-88 provides guidance on media sanitization. The National Security Agency also provides media sanitization guidance and maintains a listing of approved sanitization products at <a href="http://www.nsa.gov/ia/government/mdg.cfm">http://www.nsa.gov/ia/government/mdg.cfm</a> .	(1) The organization tracks, documents, and verifies media sanitization and disposal actions. (2) The organization periodically tests sanitization equipment and procedures to verify correct performance.	
PE-1 Physical and Environmental Protection Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	The physical and environmental protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The physical and environmental protection policy can be included as part of the general information security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.	None	
PE-2 Physical Access Authorizations	The organization 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) and issues appropriate authorization credentials. Designated officials within the organization review and approve the access list and authorization credentials [Assignment: organization-defined frequency, at least annually].	Appropriate authorization credentials include, for example, badges, identification cards, and smart cards. The organization promptly removes from the access list personnel no longer requiring access to the facility where the information system resides.	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
PE-3 Physical Access Control	The organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. The organization controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.	The organization uses physical access devices (e.g., keys, locks, combinations, card readers) and/or guards to control entry to facilities containing information systems. The organization secures keys, combinations, and other access devices and inventories those devices regularly. The organization changes combinations and keys: (i) periodically; and (ii) when keys are lost, combinations are compromised, or individuals are transferred or terminated. Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being appropriately controlled. Where federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST Special Publication 800-73. If the token-based access control function employs cryptographic verification, the access control system conforms to the requirements of NIST Special Publication	(1) The organization controls physical access to the information system independent of the physical access controls for the facility. Enhancement Supplemental Guidance: This control enhancement, in general, applies to server rooms, communications centers, or any other areas within a facility containing large concentrations of information system components or components with a higher impact level than that of the majority of the facility. The intent is to provide an additional layer of physical security for those areas where the organization may be more vulnerable due to the concentration of information system components or the impact level of the components. The control enhancement is not intended to apply to workstations or peripheral devices that are typically dispersed throughout the facility and used routinely by organizational personnel.	
Access Control for Transmission Medium	The organization controls physical access to information system distribution and transmission lines within organizational facilities.	Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.	None	
Access Control for Display Medium	The organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.	None	None	
PE-6 Monitoring Physical Access	The organization monitors physical access to the information system to detect and respond to physical security incidents.	The organization reviews physical access logs periodically and investigates apparent security violations or suspicious physical access activities. Response to detected physical security incidents is part of the organization's incident response capability.	(1) The organization monitors real-time physical intrusion alarms and surveillance equipment. (2) The organization employs automated mechanisms to recognize potential intrusions and initiate appropriate response actions.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
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.	Government contractors and others with permanent authorization credentials are not considered visitors. Personal Identity Verification (PIV) credentials for federal employees and contractors conform to FIPS 201, and the issuing organizations for the PIV credentials are accredited in accordance with the provisions of NIST Special Publication 800-79.	(1) The organization escorts visitors and monitors visitor activity, when required.	
PE-8 Access Records	The organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization review the visitor access records [Assignment: organization-defined frequency].	None	(1) The organization employs automated mechanisms to facilitate the maintenance and review of access records. (2) The organization maintains a record of all physical access, both visitor and authorized individuals.	
Power Equipment and Power Cabling	The organization protects power equipment and power cabling for the information system from damage and destruction.	None	(1) The organization employs redundant and parallel power cabling paths.	
Emergency Shutoff	The organization provides, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.	Facilities containing concentrations of information system resources may include, for example, data centers, server rooms, and mainframe rooms.	(1) The organization protects the emergency power-off capability from accidental or unauthorized activation.	
Emergency Power	The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.	None	(1) The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source. (2) The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
PE-12 Emergency Lighting	The organization employs and maintains automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes.	None	None	
PE-13 Fire Protection	The organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.	Fire suppression and detection devices/systems include, but are not limited to, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.	(1) The organization employs fire detection devices/systems that activate automatically and notify the organization and emergency responders in the event of a fire. (2) The organization employs fire suppression devices/systems that provide automatic notification of any activation to the organization and emergency responders. (3) The organization employs an automatic fire suppression capability in facilities that are not staffed on a continuous basis.	
PE-14 Temperature and Humidity Controls	The organization regularly maintains, within acceptable levels, and monitors the temperature and humidity within the facility where the information system resides.	None	None	
PE-15 Water Damage Protection	The organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.	None	(1) The organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a significant water leak.	
PE-16 Delivery and Removal	The organization authorizes and controls information system-related items entering and exiting the facility and maintains appropriate records of those items.	The organization controls delivery areas and, if possible, isolates the areas from the information system and media libraries to avoid unauthorized physical access.	None	
Alternate Work Site	The organization employs appropriate management, operational, and technical information system security controls at alternate work sites.	The organization provides a means for employees to communicate with information system security staff in case of security problems. NIST Special Publication 800-46 provides guidance on security in telecommuting and broadband communications.	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
Location of Information System Components	The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electrical interference, and electromagnetic radiation. Whenever possible, the organization also considers the location or site of the facility with regard to physical and environmental hazards.	(1) The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.	
Information Leakage	The organization protects the information system from information leakage due to electromagnetic signals emanations.	The FIPS 199 security categorization (for confidentiality) of the information system and organizational security policy guides the application of safeguards and countermeasures employed to protect the information system against information leakage due to electromagnetic signals emanations.	None	
PL-1 Security Planning Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.	The security planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security planning policy addresses the overall policy requirements for confidentiality, integrity, and availability and can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-18 provides guidance on security planning. NIST Special Publication 800-12 provides guidance on security policies and procedures.	None	
PL-2 System Security Plan	The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.	The security plan is aligned with the organization's information system architecture and information security architecture. NIST Special Publication 800-18 provides guidance on security planning.	None	
PL-3 System Security Plan Update	The organization reviews the security plan for the information system [Assignment: organization-defined frequency, at least annually] and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.	Significant changes are defined in advance by the organization and identified in the configuration management process. NIST Special Publication 800-18 provides guidance on security plan updates.	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
PL-4 Rules of Behavior	The organization establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.	Electronic signatures are acceptable for use in acknowledging rules of behavior unless specifically prohibited by organizational policy. NIST Special Publication 800-18 provides guidance on preparing rules of behavior.	None	
PL-5 Privacy Impact Assessment	The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.	OMB Memorandum 03-22 provides guidance for implementing the privacy provisions of the E-Government Act of 2002.	None	
Security-Related Activity Planning	The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.	Routine security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing/exercises. Organizational advance planning and coordination includes both emergency and non-emergency (i.e., routine) situations.	None	
PS-1 Personnel Security Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	The personnel security policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

<b>Reference Mapping Standard (800-53)</b>	<b>Title (Security Control)</b>	<b>Checklist Item / Question</b>	<b>Supplemental Guidance</b>	<b>Comments</b>
PS-2 Position Categorization	The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations [Assignment: organization-defined frequency].	Position risk designations are consistent with 5 CFR 731.106(a) and Office of Personnel Management policy and guidance.	None	
PS-3 Personnel Screening	The organization screens individuals requiring access to organizational information and information systems before authorizing access.	Screening is consistent with: (i) 5 CFR 731.106; (ii) Office of Personnel Management policy, regulations, and guidance; (iii) organizational policy, regulations, and guidance; (iv) FIPS 201 and Special Publications 800-73, 800-76, and 800-78; and (v) the criteria established for the risk designation of the assigned position.	None	
PS-4 Personnel Termination	The organization, upon termination of individual employment, terminates information system access, conducts exit interviews, retrieves all organizational information system-related property, and provides appropriate personnel with access to official records created by the terminated employee that are stored on organizational information systems.	Information system-related property includes, for example, keys, identification cards, and building passes. Timely execution of this control is particularly essential for employees or contractors terminated for cause.	None	
PS-5 Personnel Transfer	The organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization and initiates appropriate actions.	Appropriate actions that may be required include: (i) returning old and issuing new keys, identification cards, building passes; (ii) closing old accounts and establishing new accounts; (iii) changing system access authorizations; and (iv) providing for access to official records created or controlled by the employee at the old work location and in the old accounts.	None	
PS-6 Access Agreements	The organization completes appropriate signed access agreements for individuals requiring access to organizational information and information systems before authorizing access and reviews/updates the agreements [Assignment: organization-defined frequency].	Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy.	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
PS-7 Third-Party Personnel Security	The organization establishes personnel security requirements including security roles and responsibilities for third-party providers and monitors provider compliance.	Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. The organization explicitly includes personnel security requirements in acquisition-related documents. NIST Special Publication 800-35 provides guidance on information technology security services.	None	
PS-8 Personnel Sanctions	The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.	The sanctions process is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The sanctions process can be included as part of the general personnel policies and procedures for the organization.	None	
RA-1 Risk Assessment Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	The risk assessment policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publications 800-30 provides guidance on the assessment of risk. NIST Special Publication 800-12 provides guidance on security policies and procedures.	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
RA-2 Security Categorization	The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations.	The applicable federal standard for security categorization of nonnational security information and information systems is FIPS 199. The organization conducts FIPS 199 security categorizations as an organization-wide activity with the involvement of the chief information officer, senior agency information security officer, information system owners, and information owners. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and restricting or prohibiting network access in accordance with an organizational assessment of risk. NIST Special Publication 800-60 provides guidance on determining the security categories of the information types resident on the information system. Related security controls: MP-4, SC-7.	None	
RA-3 Risk Assessment	The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties).	Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk posed to organizational operations, organizational assets, or individuals based on the operation of the information system. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. Risk assessments also take into account risk posed to organizational operations, organizational assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public ac	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
RA-4 Risk Assessment Update	The organization updates the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.	The organization develops and documents specific criteria for what is considered significant change to the information system. NIST Special Publication 800-30 provides guidance on conducting risk assessment updates.	None	
Vulnerability Scanning	The organization scans for vulnerabilities in the information system [Assignment: organization-defined frequency] or when significant new vulnerabilities potentially affecting the system are identified and reported.	Vulnerability scanning is conducted using appropriate scanning tools and techniques. The organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. Vulnerability scans are scheduled and/or random in accordance with organizational policy and assessment of risk. The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems. Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, source code reviews, static analysis of source code). NIST Special Publication 800-42 provides guidance on network security testing. NIST Special Publication 800-40 (Version 2) provides guidance on patch and vulnerability management.	(1) The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned. (2) The organization updates the list of information system vulnerabilities scanned [Assignment: organization-defined frequency] or when significant new vulnerabilities are identified and reported. (3) The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of scan coverage, including vulnerabilities checked and information system components scanned.	
SA-1 System and Services Acquisition Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) 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 (ii) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	The system and services acquisition policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
SA-2 Allocation of Resources	The organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system.	The organization includes the determination of security requirements for the information system in mission/business case planning and establishes a discrete line item for information system security in the organization's programming and budgeting documentation. NIST Special Publication 800-65 provides guidance on integrating security into the capital planning and investment control process.	None	
SA-3 Life Cycle Support	The organization manages the information system using a system development life cycle methodology that includes information security considerations.	NIST Special Publication 800-64 provides guidance on security considerations in the system development life cycle.	None	
SA-4 Acquisitions	The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.	<p>Solicitation Documents</p> <p>The solicitation documents (e.g., Requests for Proposals) for information systems and services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (security needs and, as necessary, specific security controls and other specific FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. The requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. NIST Special Publication 800-36 provides guidance on the selection of information security products. NIST Special Publication 800-35 provides guidance on information technology security services. NIST Special Publication 800-64 provides guidance on security considerations in the system development life cycle.</p> <p>Information System Documentation</p> <p>The solicitation documents include requirements for appropriate information system documentation. The documentation includes:</p> <p>Use of Tested, Evaluated, and Validated Products</p> <p>NIST Special Publication 800-23 provides guidance on the Configuration Settings and Implementation Guidance</p> <p>The information system required documentation includes:</p>	<p>(1)</p> <p>The organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.</p> <p>(2)</p> <p>The organization requires in solicitation documents that appropriate documentation be provided describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).</p>	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
SA-5 Information System Documentation	The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.	Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non-existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed.	(1) The organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls. (2) The organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).	
SA-6 Software Usage Restrictions	The organization complies with software usage restrictions.	Software and associated documentation are used in accordance with contract agreements and copyright laws. For software and associated documentation protected by quantity licenses, the organization employs tracking systems to control copying and distribution. The organization controls and documents the use of publicly accessible 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.	None	
SA-7 User Installed Software	The organization enforces explicit rules governing the installation of software by users.	If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software that is free only for personal, not government use, and software whose pedigree with regard to being potentially malicious is unknown or suspect).	None	
Security Engineering Principles	The organization designs and implements the information system using security engineering principles.	NIST Special Publication 800-27 provides guidance on engineering principles for information system security. The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the system.	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
SA-9 External Information System Services	The organization: (i) requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements; and (ii) monitors security control compliance.	An external information system service is a service that is implemented outside of the accreditation boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. Ultimately, the responsibility for adequately mitigating risks to the organization's operations and assets, and to individuals, arising from the use of external information system services remains with the authorizing official. Authorizing officials must require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information system security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of	None	
Developer Configuration Management	The organization requires that information system developers create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.	This control also applies to the development actions associated with information system changes.	None	
Developer Security Testing	The organization requires that information system developers create a security test and evaluation plan, implement the plan, and document the results.	Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security certification and accreditation process for the delivered information system. Related security controls: CA-2, CA-4.	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
SC-1 System and Communications Protection Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.	The system and communications protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.	None	
Application Partitioning	The information system separates user functionality (including user interface services) from information system management functionality.	The information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.	None	
Security Function Isolation	The information system isolates security functions from nonsecurity functions.	The information system isolates security functions from nonsecurity functions by means of partitions, domains, etc., including control of access to and integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process.	<p>(1) The information system employs underlying hardware separation mechanisms to facilitate security function isolation.</p> <p>(2) The information system isolates critical security functions (i.e., functions enforcing access and information flow control) from both nonsecurity functions and from other security functions.</p> <p>(3) The information system minimizes the number of nonsecurity functions included within the isolation boundary containing security functions.</p> <p>(4) The information system security functions are implemented as largely independent modules that avoid unnecessary interactions between modules.</p> <p>(5) The information system security functions are implemented as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.</p>	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
Information Remnance	The information system prevents unauthorized and unintended information transfer via shared system resources.	Control of information system remnance, sometimes referred to as object reuse, or data remnance, prevents information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system.	None	
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].	A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Information systems that are publicly accessible can be protected by employing increased capacity and bandwidth combined with service redundancy.	(1) The information system restricts the ability of users to launch denial of service attacks against other information systems or networks. (2) The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.	
Resource Priority	The information system limits the use of resources by priority.	Priority protection helps prevent a lower-priority process from delaying or interfering with the information system servicing any higher-priority process.	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
SC-7 Boundary Protection	The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.	Any connections to the Internet, or other external networks or information systems, occur through managed interfaces consisting of appropriate boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels) arranged in an effective architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ). Information system boundary protections at any designated alternate processing sites provide the same levels of protection as that of the primary site. As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and applying the concepts of managed interfaces described above to restrict or prohibit network access in accordance with an organizational assessment of risk. FIPS 199 security categorization guides the selection of appropriate candidates for domain partitioning. The organization carefully considers the intrinsically shared nature of commercial telecommunications services	(1) The organization physically allocates publicly accessible information system components to separate subnetworks with separate, physical network interfaces. Enhancement Supplemental Guidance: Publicly accessible information system components include, for example, public web servers. (2) The organization prevents public access into the organization's internal networks except as appropriately mediated. (3) The organization limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic. (4) The organization implements a managed interface (boundary protection devices in an effective security architecture) with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted. (5) The information system denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception). (6) The organization prevents the unauthorized release of information outside of the information system boundary.	
Transmission Integrity	The information system protects the integrity of transmitted information.	If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission integrity. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST Special Publication 800-52 provides guidance on protecting transmission integrity using Transport Layer Security (TLS). NIST Special Publication 800-77 provides guidance on protecting transmission integrity using IPsec. NIST Special Publication 800-81 provides guidance on Domain Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems.	(1) The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures. Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
Transmission Confidentiality	The information system protects the confidentiality of transmitted information.	If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST Special Publication 800-52 provides guidance on protecting transmission confidentiality using Transport Layer Security (TLS). NIST Special Publication 800-77 provides guidance on protecting transmission confidentiality using IPsec. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems. Related security control: AC-17.	(1) The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures. Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems.	
Network Disconnect	The information system terminates a network connection at the end of a session or after [Assignment: organization-defined time period] of inactivity.	The organization applies this control within the context of risk management that considers specific mission or operational requirements.	None	
Trusted Path	The information system establishes a trusted communications path between the user and the following security functions of the system: [Assignment: organization-defined security functions to include at a minimum, information system authentication and reauthentication].	A trusted path is employed for high-confidence connections between the security functions of the information system and the user (e.g., for login).	None	
Cryptographic Key Establishment and Management	When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.	NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management.	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
SC-13 Use of Cryptography	For information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.	The applicable federal standard for employing cryptography in nonnational security information systems is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. NIST Special Publications 800-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management. Additional information on the use of validated cryptography is available at <a href="http://csrc.nist.gov/cryptval">http://csrc.nist.gov/cryptval</a> .	None	
SC-14 Public Access Protections	The information system protects the integrity and availability of publicly available information and applications.	None	None	
Collaborative Computing	The information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.	Collaborative computing mechanisms include, for example, video and audio conferencing capabilities. Explicit indication of use includes, for example, signals to local users when cameras and/or microphones are activated.	(1) The information system provides physical disconnect of camera and microphone in a manner that supports ease of use.	
Transmission of Security Parameters	The information system reliably associates security parameters with information exchanged between information systems.	Security parameters include, for example, security labels and markings. Security parameters may be explicitly or implicitly associated with the information contained within the information system.	None	
Public Key Infrastructure Certificates	The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.	For user certificates, each agency either establishes an agency certification authority cross-certified with the Federal Bridge Certification Authority at medium assurance or higher or uses certificates from an approved, shared service provider, as required by OMB Memorandum 05-24. NIST Special Publication 800-32 provides guidance on public key technology. NIST Special Publication 800-63 provides guidance on remote electronic authentication.	None	
Mobile Code	The organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and controls the use of mobile code within the information system.	Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Control procedures prevent the development, acquisition, or introduction of unacceptable mobile code within the information system. NIST Special Publication 800-28 provides guidance on active content and mobile code.	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
Voice Over Internet Protocol	The organization: (i) establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and controls the use of VoIP within the information system.	NIST Special Publication 800-58 provides guidance on security considerations for VoIP technologies employed in information systems.	None	
Secure Name / Address Resolution Service (Authoritative Source)	The information system that provides name/address resolution service provides additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries.	This control enables remote clients to obtain origin authentication and integrity verification assurances for the name/address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service; digital signatures and cryptographic keys are examples of additional artifacts; and DNS resource records are examples of authoritative data. NIST Special Publication 800-81 provides guidance on secure domain name system deployment.	(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. Enhancement Supplemental Guidance: An example means to indicate the security status of child subspaces is through the use of delegation signer resource records.	
Secure Name / Address Resolution Service (Recursive or Caching Resolver)	The information system that provides name/address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.	A resolving or caching domain name system (DNS) server is an example of an information system that provides name/address resolution service for local clients and authoritative DNS servers are examples of authoritative sources. NIST Special Publication 800-81 provides guidance on secure domain name system deployment.	(1) The information system performs data origin authentication and data integrity verification on all resolution responses whether or not local clients explicitly request this service. Enhancement Supplemental Guidance: Local clients include, for example, DNS stub resolvers.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
Architecture and Provisioning for Name / Address Resolution Service	The information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation.	A domain name system (DNS) server is an example of an information system that provides name/address resolution service. To eliminate single points of failure and to enhance redundancy, there are typically at least two authoritative domain name system (DNS) servers, one configured as primary and the other as secondary. Additionally, the two servers are commonly located in two different network subnets and geographically separated (i.e., not located in the same physical facility). If organizational information technology resources are divided into those resources belonging to internal networks and those resources belonging to external networks, authoritative DNS servers with two roles (internal and external) are established. The DNS server with the internal role provides name/address resolution information pertaining to both internal and external information technology resources while the DNS server with the external role only provides name/address resolution information pertaining to external information technology resources. The list of clients who can access the authoritative DNS server of a particular role is also spe	None	
Session Authenticity	The information system provides mechanisms to protect the authenticity of communications sessions.	This control focuses on communications protection at the session, versus packet, level. The intent of this control is to implement session-level protection where needed (e.g., in service-oriented architectures providing web-based services). NIST Special Publication 800-52 provides guidance on the use of transport layer security (TLS) mechanisms. NIST Special Publication 800-77 provides guidance on the deployment of IPsec virtual private networks (VPNs) and other methods of protecting communications sessions. NIST Special Publication 800-95 provides guidance on secure web services.	None	
SI-1 System and Information Integrity Policy and Procedures	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.	The system and information integrity policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
SI-2 Flaw Remediation	The organization identifies, reports, and corrects information system flaws.	The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws). The organization (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) promptly installs newly released security relevant patches, service packs, and hot fixes, and tests patches, service packs, and hot fixes for effectiveness and potential side effects on the organization's information systems before installation. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling are also addressed expeditiously. Flaw remediation is incorporated into configuration management as an emergency change. NIST Special Publication 800-40, provides guidance on security patch installation and patch management. Related security controls: CA-2, CA-4, CA-7, CM-3, IR-4, SI-11.	(1) The organization centrally manages the flaw remediation process and installs updates automatically. (2) The organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation.	
SI-3 Malicious Code Protection	The information system implements malicious code protection.	The organization employs malicious code protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the malicious code protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware) transported: (i) by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., USB devices, diskettes or compact disks), or other common means; or (ii) by exploiting information system vulnerabilities. The organization updates malicious code protection mechanisms (including the latest virus definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures. The organization considers using malicious code protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). The organization also considers the receipt	(1) The organization centrally manages malicious code protection mechanisms. (2) The information system automatically updates malicious code protection mechanisms.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
Information System Monitoring Tools and Techniques	The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.	Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). Monitoring devices are strategically deployed within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect essential information. Monitoring devices are also deployed at ad hoc locations within the system to track specific transactions. Additionally, these devices are used to track the impact of security changes to the information system. The granularity of the information collected is determined by the organization based upon its monitoring objectives and the capability of the information system to support such activities. Organizations consult appropriate legal counsel with regard to all information system monitoring activities. Organizations heighten the level of information system monitoring activity whenever there is an indication of incre	(1) The organization interconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using common protocols. (2) The organization employs automated tools to support near-real-time analysis of events. (3)The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination. (4)The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions. Enhancement Supplemental Guidance: Unusual/unauthorized activities or conditions include, for example, the presence of malicious code, the unauthorized export of information, or signaling to an external information system. (5)The information system provides a real-time alert when the following indications of compromise or potential compromise occur: [Assignment: organization-defined list of compromise indicators].	
SI-5 Security Alerts and Advisories	The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.	The organization documents the types of actions to be taken in response to security alerts/advisories. The organization also maintains contact with special interest groups (e.g., information security forums) that: (i) facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies); (ii) provide access to advice from security professionals; and (iii) improve knowledge of security best practices. NIST Special Publication 800-40 provides guidance on monitoring and distributing security alerts and advisories.	(1) The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.	
Security Functionality Verification	The information system verifies the correct operation of security functions [Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): notifies system administrator, shuts the system down, restarts the system] when anomalies are discovered.	The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests, the organization either implements compensating security controls or explicitly accepts the risk of not performing the verification as required.	(1) The organization employs automated mechanisms to provide notification of failed automated security tests. (2) The organization employs automated mechanisms to support management of distributed security testing.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
Software and Information Integrity	The information system detects and protects against unauthorized changes to software and information.	The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.	(1) The organization reassesses the integrity of software and information by performing [Assignment: organization-defined frequency] integrity scans of the system. (2) The organization employs automated tools that provide notification to appropriate individuals upon discovering discrepancies during integrity verification. (3) The organization employs centrally managed integrity verification tools.	
Spam Protection	The information system implements spam protection.	The organization employs spam protection mechanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail, electronic mail attachments, Internet accesses, or other common means. Consideration is given to using spam protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). NIST Special Publication 800-45 provides guidance on electronic mail security.	(1) The organization centrally manages spam protection mechanisms. (2) The information system automatically updates spam protection mechanisms.	
Information Input Restrictions	The organization restricts the capability to input information to the information system to authorized personnel.	Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.	None	
Information Accuracy, Completeness, Validity, and Authenticity	The information system checks information for accuracy, completeness, validity, and authenticity.	Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- 800-53 Controls**

Reference Mapping Standard (800-53)	Title (Security Control)	Checklist Item / Question	Supplemental Guidance	Comments
Error Handling	The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.	The structure and content of error messages are carefully considered by the organization. Error messages are revealed only to authorized personnel. Error messages generated by the information system provide timely and useful information without revealing potentially harmful information that could be used by adversaries. Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) are not listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.	None	
Information Output Handling and Retention	The organization handles and retains output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	None	None	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- HIPAA**

Final Rule Number	HIPAA Requirement	Federal Information Security Management Act Requirements	Comments
§164.308	<b>Administrative Safeguards</b>		
§164.308a1(i)	<i>Standard: Security management process.</i> Implement policies and procedures to prevent, detect, contain, and correct security violations. This includes the following:		
§164.308a1(ii)A	<u>Risk analysis (Required).</u> Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity	1.1 Critical Element: Is risk periodically assessed? 1.1.1 Is the current system configuration documented, including links to other systems? 1.1.2 Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change? 1.1.3 Has data sensitivity and integrity of the data been considered? 1.1.4 Have threat sources, both natural and manmade, been identified? 1.1.5 Has a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat sources been developed and maintained current? 1.1.6 Has an analysis been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities?	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- HIPAA**

Final Rule Number	HIPAA Requirement	Federal Information Security Management Act Requirements	Comments
§164.308a1(ii)B	<u>Risk management (Required).</u> Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).	1.2 Critical Element 2: Do program officials understand the risk to systems under their control and determine the acceptable level of risk? 1.2.1 Are final risk determinations and related management approvals documented and maintained on file? 1.2.2 Has a mission/business impact analysis been conducted? 1.2.3 Have additional controls been identified to sufficiently mitigate identified risks?	
§164.308a1(ii)C	<u>Sanction policy (Required).</u> Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.	6.1.5 Are mechanisms in place for holding users responsible for their actions?	
§164.308a1(ii)D	<u>Information system activity review (Required).</u> Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	2.1 Critical Element: Have the security controls of the system and interconnected systems been reviewed? 2.1.1 Has the system and all network boundaries been subjected to periodic reviews? 2.1.2 Has an independent review been performed when a significant change occurred? 2.1.3 Are routine self-assessments conducted? 2.1.4 Are tests and examinations of key controls routinely made, i.e., network scans, analyses of router and switch setting, penetration testing? 2.1.5 Are security alerts and security incidents analyzed and remedial actions taken? 2.1.6 Have the security controls been tested and evaluated in the last year?	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- HIPAA**

<b>Final Rule Number</b>	<b>HIPAA Requirement</b>	<b>Federal Information Security Management Act Requirements</b>	<b>Comments</b>
§164.308a2	<i>Standard: Assigned security responsibility.</i> Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.	13.1.8 Critical Element: Has and ISO and AISO been appointed in writing?	
§164.308a3(i)	<i>Standard: Workforce security.</i> Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.		
§164.308a3(ii)	Implementation specifications:		

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- HIPAA**

Final Rule Number	HIPAA Requirement	Federal Information Security Management Act Requirements	Comments
§164.308a3(ii)A	<u>Authorization and/or supervision (Addressable).</u> Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	6.1.1 Are all positions reviewed for sensitivity level? 6.1.2 Are there documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties? 6.1.7 Are hiring, transfer, and termination procedures established? 6.1.8 Is there a process for requesting, establishing, issuing, and closing user accounts? 6.2 Critical Element 2: Is appropriate background screening for assigned positions completed prior to granting access?	
§164.308a3(ii)B	<u>Workforce clearance procedure (Addressable).</u> Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	6.1.1 Are all positions reviewed for sensitivity level? 6.2 Critical Element 2: Is appropriate background screening for assigned positions completed prior to granting access?	
§164.308a3(ii)C	<u>Termination procedures (Addressable).</u> Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	6.1.7 Are hiring, transfer, and termination procedures established?	
§164.308a4(i)	<i>Standard: Information access management.</i>		
§164.308a4(ii)	Implementation specifications:		

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- HIPAA**

Final Rule Number	HIPAA Requirement	Federal Information Security Management Act Requirements	Comments
§164.308a4(ii)A	<p><u>Isolating health care clearinghouse functions (Required).</u> If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.</p>	<p>2.1 Critical Element: Have the security controls of the system and interconnected systems been reviewed? 2.1.1 Has the system and all network boundaries been subjected to periodic reviews? 3.2.9 If the system connects to other systems, have controls been established and disseminated to the owners of the interconnected systems? 4.1.8 Has management authorized interconnections to all systems (including systems owned and operated by another program, agency, organization or contractor)? 5.1 Critical Element: Is a system security plan documented for the system and all interconnected systems if the boundary controls are ineffective? 12.2.3 Are there written agreements regarding how data is shared between interconnected systems? 14.2.1 Is incident information and common vulnerabilities or threats shared with interconnected systems?</p>	
§164.308a4(ii)B	<p><u>Access authorization (Addressable).</u> Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.</p>	<p>15.1.1 Is a current list maintained and approved of authorized users and their access? 16.1 Critical Element: Do the logical access controls restrict users to authorized transactions and functions?</p>	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- HIPAA**

Final Rule Number	HIPAA Requirement	Federal Information Security Management Act Requirements	Comments
§164.308a4(ii)C	<p><u>Access establishment and modification (Addressable).</u> Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.</p>	<p>15.1.5 Critical Element: Are personnel files matched with user accounts to ensure that terminated or transferred individuals do not retain system access? 15.1.8 Are inactive user identifications disabled after a specified period of time? 15.2.2 Do data owners periodically review access authorization listings to determine whether they remain appropriate?</p>	
§164.308a5(i)	<p><i>Standard: Security awareness and training.</i> Implement a security awareness and training program for all members of its workforce (including management).</p>		
§164.308a5(ii)	<p>Implementation specifications. Implement:</p>		
§164.308a5(ii)A	<p><u>Security reminders (Addressable).</u> Periodic security updates.</p>	<p>13.1.4 Are methods employed to make employees aware of security, i.e., posters, booklets?</p>	
§164.308a5(ii)B	<p><u>Protection from malicious software (Addressable).</u> Procedures for guarding against, detecting, and reporting malicious software.</p>	<p>10.2.13 Is the use of copyrighted software or shareware and personally owned software/equipment documented? 11.1 Critical Element: Is virus detection and elimination software installed and activated? 11.2.2 Is inappropriate or unusual activity reported, investigated, and appropriate actions taken?</p>	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- HIPAA**

Final Rule Number	HIPAA Requirement	Federal Information Security Management Act Requirements	Comments
§164.308a5(ii)C	<u>Log-in monitoring (Addressable).</u> Procedures for monitoring log-in attempts and reporting discrepancies.	16.1.10 Is access monitored to identify apparent security violations and are such events investigated? 16.2 Critical Element: Are there logical controls over network access? 16.2.5 Are network activity logs maintained and reviewed?	
§164.308a5(ii)D	<u>Password management (Addressable).</u> Procedures for creating, changing, and safeguarding passwords	13.1.1 Have employees received a copy of the rules of behavior? 13.1.5 Have employees received a copy of or have easy access to agency security procedures and policies? 15.1.6 Are passwords changed at least every ninety days or earlier if needed? 15.1.7 Do passwords require alpha numeric, upper/lower case, and special characters? 15.1.9 Are passwords not displayed when entered? 15.1.10 Are there procedures in place for handling lost and compromised passwords? 15.1.11 Are passwords distributed securely and users informed not to reveal their passwords to anyone (social engineering)? 15.1.12 Are passwords transmitted and stored using secure protocols/algorithms?	
§164.308a6(i)	<i>Standard: Security incident procedures.</i> Implement policies and procedures to address security incidents.		

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- HIPAA**

Final Rule Number	HIPAA Requirement	Federal Information Security Management Act Requirements	Comments
§164.308a6(ii)	<p>Implementation specification: <u>Response and Reporting (Required)</u>. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.</p>	<p>14.1.1 Is a formal incident response capability available? 14.1.2 Is there a process for reporting incidents? 14.1.3 Are incidents monitored and tracked until resolved? 14.1.4 Are personnel trained to recognize and handle incidents? 14.1.5 Are alerts/advisories received and responded to? 14.1.6 Is there a process to modify incident handling procedures and control techniques after an incident occurs?</p>	
§164.308a7(i)	<p><i>Standard: Contingency plan.</i> Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information</p>		
§164.308a7(ii)	Implementation specifications:		

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- HIPAA**

Final Rule Number	HIPAA Requirement	Federal Information Security Management Act Requirements	Comments
§164.308a7(ii)A	<p><u>Data backup plan (Required).</u> Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.</p>	<p>9.1.1 Are critical data files and operations identified and the frequency of file backup documented? 9.2.5 Critical Element: Are backups stored in a secure, off-site location which is identified in the contingency plan? 9.2.6 Are backup files created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged? 9.2.8 Are all system defaults reset after being restored from a backup? 9.2.9 Are the backup storage site and alternate site geographically removed from the primary site and physically protected?</p>	
§164.308a7(ii)B	<p><u>Disaster recovery plan (Required).</u> Establish (and implement as needed) procedures to restore any loss of data.</p>	<p>9.2 Critical Element: Has a comprehensive contingency plan been developed and documented? 9.2.2 Are responsibilities for recovery assigned? 9.2.3 Are there detailed instructions for restoring operations? 9.2.10 Has the contingency plan been distributed to all appropriate personnel? 9.3 Critical Element 3: Are tested contingency/disaster recovery plans in place</p>	
§164.308a7(ii)C	<p><u>Emergency mode operation plan (Required).</u> Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.</p>	<p>9.2.4 Is there an alternate processing site; if so, is there a contract or interagency agreement in place?</p>	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- HIPAA**

Final Rule Number	HIPAA Requirement	Federal Information Security Management Act Requirements	Comments
§164.308a7(ii)D	<p><u>Testing and revision procedures (Addressable).</u> Implement procedures for periodic testing and revision of contingency plans.</p>	<p>9.3 Critical Element 3: Are tested contingency/disaster recovery plans in place? 9.3.1 Is an up-to-date copy of the plan stored securely off-site? 9.3.2 Are employees trained in their roles and responsibilities? 9.3.3 Is the plan periodically tested and readjusted as appropriate? 9.3.4 Has the contingency plan been tested in the past year?</p>	
§164.308a7(ii)E	<p><u>Applications and data criticality analysis (Addressable).</u> Assess the relative criticality of specific applications and data in support of other contingency plan components.</p>	<p>9.1 Critical Element: Have the most critical and sensitive operations and their supporting computer resources been identified? 9.1.2 Are resources supporting critical operations identified? 9.1.3 Have processing priorities been established and approved by management?</p>	
§164.308a8	<p><i>Standard: Evaluation.</i> Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart</p>	<p>2.1 Critical Element: Have the security controls of the system and interconnected systems been reviewed? 2.1.5 Are security alerts and security incidents analyzed and remedial actions taken? 2.2.1 Is there an effective and timely process for reporting significant weakness and ensuring effective remedial action?</p>	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- HIPAA**

Final Rule Number	HIPAA Requirement	Federal Information Security Management Act Requirements	Comments
§164.308a8b1	<p><i>Standard: Business associate contracts and other arrangements.</i></p> <p>A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information.</p>		
§164.308a8b4	<p>Implementation specifications: <u>Written contract or other arrangement (Required)</u>. Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).</p>	<p>3.1.8 Is there a written agreement with program officials on the security controls employed and residual risk?</p> <p>12.2.3 Are there written agreements regarding how data is shared between interconnected systems?</p>	
§164.310	<p>Physical safeguards.</p> <p>A covered entity must, in accordance with § 164.306:</p>		

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- HIPAA**

Final Rule Number	HIPAA Requirement	Federal Information Security Management Act Requirements	Comments
§164.310a1	<i>Standard: Facility access controls.</i> Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.		
§164.310a2	Implementation specifications:		
§164.310a2(i)	<u>Contingency operations (Addressable).</u> Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	7.1.6 Do emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter after fire drills, etc?	
§164.310a2(ii)	<u>Facility security plan (Addressable).</u> Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	7.1 Critical Element: Have adequate physical security controls been implemented that are commensurate with the risks of physical damage or access?	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- HIPAA**

Final Rule Number	HIPAA Requirement	Federal Information Security Management Act Requirements	Comments
§164.310a2(iii)	<p><u>Access control and validation procedures (Addressable).</u> Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.</p>	<p>7.1.1 Is access to facilities controlled through the use of guards, identification badges, or entry devices such as key cards? 7.1.2 Does management regularly review the list of persons with physical access to sensitive facilities? 7.1.5 Are unused keys or other entry devices secured? 7.1.7 Are visitors to sensitive areas signed in and escorted? 7.1.9 Are physical accesses monitored through audit trails and apparent security violations investigated and remedial action taken? 7.1.11 Are visitors, contractors and maintenance personnel authenticated through the use of preplanned appointments and identification checks? 10.1.1 Are restrictions in place on who performs maintenance and repair activities?</p>	
§164.310a2(iv)	<p><u>Maintenance records (Addressable).</u> Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).</p>	<p>7.1.11 Are visitors, contractors and maintenance personnel authenticated through the use of preplanned appointments and identification checks? 7.1.14 Are heating and air-conditioning systems regularly maintained? 10.1.1 Are restrictions in place on who performs maintenance and repair activities?</p>	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- HIPAA**

Final Rule Number	HIPAA Requirement	Federal Information Security Management Act Requirements	Comments
§164.310b	<p><i>Standard: Workstation use.</i> Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.</p>	4.1.3 Have Rules of Behavior been established and signed by users?	
§164.310c	<p><i>Standard: Workstation security.</i> Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.</p>	7.2.1 Are computer monitors located to eliminate viewing by unauthorized persons? 7.3.2 Are portable systems stored securely? 15.1 Critical Element 1: Are users individually authenticated via passwords, tokens, or other means? 15.1.14 Is there a limit to the number of invalid access attempts that may occur for a given user? 16.1.4 Do workstations disconnect or screen savers lock system after a specific period of inactivity?	
§164.310d1	<p><i>Standard: Device and media controls.</i> Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.</p>		
§164.310d2	Implementation specifications:		

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- HIPAA**

Final Rule Number	HIPAA Requirement	Federal Information Security Management Act Requirements	Comments
§164.310d2(i)	<u>Disposal (Required).</u> Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	3.2.12 Is information or media purged, overwritten, degaussed, or destroyed when disposed or used elsewhere? 8.2.9 Is damaged media stored and destroyed? 8.2.10 Is hardcopy media shredded or destroyed when no longer needed?	
§164.310d2(ii)	<u>Media re-use (Required).</u> Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.	3.2.12 Is information or media purged, overwritten, degaussed, or destroyed when disposed or used elsewhere? 8.2.8 Is media sanitized for reuse?	
§164.310d2(iii)	<u>Accountability (Addressable).</u> Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	3.2.12 Is information or media purged, overwritten, degaussed, or destroyed when disposed or used elsewhere? 8.2.8 Is media sanitized for reuse? 3.2.13 Is a record kept of who implemented the disposal actions and verified that the information or media was sanitized? 8.2.3 Are audit trails used for receipt of sensitive inputs/outputs? 8.2.4 Are controls in place for transporting or mailing media or printed output? 8.2.7 Are audit trails kept for inventory management? 8.2.11 Critical Element: Does a responsible facility official certify that sensitive data has been removed from equipment with storage media before disposing of the equipment?	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- HIPAA**

Final Rule Number	HIPAA Requirement	Federal Information Security Management Act Requirements	Comments
§164.310d2(iv)	<p><u>Data backup and storage (Addressable).</u> Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.</p>	<p>9.1.1 Are critical data files and operations identified and the frequency of file backup documented? 9.2.5 Critical Element: Are backups stored in a secure, off-site location which is identified in the contingency plan? 9.2.6 Are backup files created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged? 9.2.8 Are all system defaults reset after being restored from a backup? 9.2.9 Are the backup storage site and alternate site geographically removed from the primary site and physically protected? 10.1.3 Are there on-site and off-site maintenance procedures (e.g. , escort of maintenance personnel, sanitization of devices removed from the site)?</p>	
§164.312	<p>Technical safeguards. A covered entity must, in accordance with § 164.306:</p>		
§164.312a1	<p><i>Standard: Access control.</i> Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).</p>		
§164.312a2	<p>Implementation specifications:</p>		

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- HIPAA**

Final Rule Number	HIPAA Requirement	Federal Information Security Management Act Requirements	Comments
§164.312a2(i)	<u>Unique user identification (Required).</u> Assign a unique name and/or number for identifying and tracking user identity.	15.1 Critical Element 1: Are users individually authenticated via passwords, tokens, or other means? 15.2.1 Does the system correlate actions to users?	
§164.312a2(ii)	<u>Emergency access procedure (Required).</u> Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency	15.1.4 Is emergency and temporary access authorized?	
§164.312a2(iii)	<u>Automatic logoff (Addressable).</u> Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	16.1.4 Do workstations disconnect or screen savers lock system after a specific period of inactivity?	
§164.312a2(iv)	<u>Encryption and decryption (Addressable).</u> Implement a mechanism to encrypt and decrypt electronic protected health information.	7.3.1 Are sensitive data files encrypted on all portable systems? 16.1.7 If encryption is used, does it meet federal standards? 16.1.8 If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving?	
§164.312b	<i>Standard: Audit controls.</i> Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	17.1 Critical Element: Is activity involving access to and modification of sensitive or critical files logged, monitored, and possible security violations investigated?	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- HIPAA**

Final Rule Number	HIPAA Requirement	Federal Information Security Management Act Requirements	Comments
§164.312c1	<p><i>Standard: Integrity.</i> Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.</p>		
§164.312c2	<p>Implementation specification: <u>Mechanism to authenticate electronic protected health information (Addressable).</u> Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.</p>	<p>11.2 Critical Element: Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended?</p>	
§164.312d	<p><i>Standard: Person or entity authentication.</i> Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.</p>	<p>15.1 Critical Element 1: Are users individually authenticated via passwords, tokens, or other means?</p>	
§164.312e1	<p><i>Standard: Transmission security.</i> Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.</p>		
§164.312e2	<p>Implementation specifications:</p>		

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- HIPAA**

<b>Final Rule Number</b>	<b>HIPAA Requirement</b>	<b>Federal Information Security Management Act Requirements</b>	<b>Comments</b>
§164.312e2(i)	<u>Integrity controls (Addressable).</u> Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of	11.2 Critical Element: Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended?	
§164.312e2(ii)	<u>Encryption (Addressable).</u> Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	16.1.7 If encryption is used, does it meet federal standards?	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- Privacy Checklist**

Reference to VA Policy	Document Section	Checklist Item / Question	Comments
VA Directive 6502	1.1	Is the Privacy Officer's office secure during regular business hours?	
VA Directive 6502	1.2	Does the Privacy Officer maintain files that contain individually identifiable information including complaint investigation information in his/her office?	
VA Directive 6502	1.3	Is there appropriate limited access to the privacy office outside of working hours?	
VA Directive 6502	1.4	Is unauthorized access to individually identifiable information reported to the privacy or security officer?	
VA Directive 6502	1.5	Are computer monitors in public areas positioned to avoid observation by visitors?	
VA Directive 6502	1.5a	Are privacy screens used as appropriate?	
VA Directive 6502	1.6	Are partitions or movable dividers placed between patient admissions/eligibility/ registration areas?	
VA Directive 6502	1.7	Are patient names and appointment times the only information requested on sign-in sheets in clinics?	
VA Directive 6502	1.8	Do employees keep their voices low when discussing IIHI with other members of the workforce or families?	
VA Directive 6502	1.9	Is dictation completed in areas where IIHI cannot be overheard by unauthorized people?	
VA Directive 6502	1.1	Do members of the workforce hold telephone conversations or use speakerphones only in areas where IIHI may not be overheard?	
VA Directive 6502	1.11	If speakerphones are used, are volume levels kept low to avoid unauthorized workforce, visitors or patients from overhearing IIHI?	
VA Directive 6502	1.12	Are medical charts and other documents containing IIHI placed face-down or concealed from direct observation?	
VA Directive 6502	1.13	What IIHI is written for reference related to patient care, status or identification on whiteboards that can be seen by unauthorized workforce members, visitors or patients?	
VA Directive 6502	1.14	Does your facility maintain bingo boards in the pharmacy or other public areas?	
VA Directive 6502	1.15	If bingo boards are used, what information is displayed on bingo boards?	
VA Directive 6502	1.16	Are faxes containing IIHI removed immediately upon completion of transmission?	
VA Directive 6502	1.17	Are fax machines located in secure and/or protected areas, away from unauthorized people?	
VA Directive 6502	1.18	Is there a confidentiality statement on all fax cover sheets?	
VA Directive 6502	1.19	Are paper (hard) copies of patient health records located in secure areas when unattended?	
VA Directive 6502	1.2	Are electronic (CPRS/VISTA) copies of patient health records kept secure at all times?	
VA Directive 6502	1.21	Are documents/health records containing IIHI filed or stored in a way that avoids access or observation by unauthorized workforce members, patients, visitors or others?	
VA Directive 6502	1.22	Are documents/health records containing IIHI left in in/out baskets, on desks or counters on unsecured areas?	
VA Directive 6502	1.23	Are documents/health records/charts left unattended in nurse's stations or administration areas?	
VA Directive 6502	1.24	Is IIHI left unattended on printers, fax or copy machines?	
VA Directive 6502	1.25	Is mail containing IIHI that is distributed throughout the facility maintained in a secure area away from public view?	
VA Directive 6502	1.26	How is a veteran's name displayed outside their hospital room?	
VA Directive 6502	1.27	How is IIHI on wrist bracelets, IV bag labels, stickers, etc. destroyed at your facility?	
VA Directive 6502	1.28	What type of paper shredding/destruction does your facility use?	
VA Directive 6502	1.28a	Is VHA personnel available for observing and certifying shredding takes place	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- Privacy Checklist**

Reference to VA Policy	Document Section	Checklist Item / Question	Comments
VA Directive 6502	1.29	Does paper containing IIHI remain unsecured in recycle bins/shred bins or boxes under desks	
VA Directive 6502	1.3	Are recycle bins/shred bins containing IIHI emptied at the end of each day; or are they secured at the end of each day?	
VA Directive 6502	1.31	Is IIHI placed in non-shred or non-secured containers under desks at nurse's stations and provider offices?	
VA Directive 6502	1.32	Are backup methods or contingency plans specified in contracts for document destruction of IIHI when the primary method is not available?	
VA Directive 6502	1.33	Are recycle bins/shred-bins secured from unauthorized removal of IIHI?	
VA Directive 6502	1.34	What is the frequency of destruction of IIHI in recycle bins/shred bins?	
VA Directive 6502	1.35	Is the patient's name the only identifying information called in waiting room areas?	
VA Directive 6502	1.36	Check all equipment that is reasonably secure from public view or access:	
VA Directive 6502	1.38	Are all outside contractors/vendors escorted or monitored while within areas that give	
VA Directive 6502	1.39	Are workforce members wearing properly displayed identification badges at all times while on the premises as required by your facility?	
VA Directive 6502	1.39a	Are visitors questioned about identification badges when unescorted in restricted areas?	
VA Directive 6502	1.4	Is access to VISTA/CPRS provided in compliance with VHA Handbook 1605.2 (Minimum Necessary Standards)	
VA Directive 6502	2.1	If individuals are denied access to or a copy of their IIHI, are they provided with written notification with their appeal rights?	
VA Directive 6502	2.2	If your facility maintains IIHI does it allow individuals to access their records in the original form (paper chart, VISTA, etc.)?	
VA Directive 6502	2.3	If the answer to the previous question is "Yes", are individuals given a private area in which to review their records; with supervision?	
VA Directive 6502	3.1	Are amendment requests processed in accordance with VHA handbook 1605.1?	
VA Directive 6502	3.2	When an amendment is granted, are previous recipients of the data provided with an amended copy of the record?	
VA Directive 6502	3.3	Are individuals whose amendment requests are denied, provided with a written notification of their appeal rights?	
VA Directive 6502	3.4	Are denials for amendment request approved and signed by the Medical Center Director (MCD)?	
VA Directive 6502	3.5	Are all amendment requests reviewed by the health care provider who created the record or applicable appropriate level provider if the original provider is no longer available?	
VA Directive 6502	4.1	How many requests for accounting of disclosure has your facility received within the last 12 months?	
VA Directive 6502	4.2	Is there a process in place to provide an individual with an accounting of disclosure of their records?	
VA Directive 6502	4.3	Can the accounting of disclosure be provided to the veteran or authorized representative upon request?	
VA Directive 6502	4.4	Do all workforce members know where to refer an individual to obtain an accounting of disclosures of their records?	
VA Directive 6502	4.5	How long does your facility take to respond to a request for an accounting of disclosure?	
VA Directive 6502	5.1	Is there a local policy for managing the facility directory?	
VA Directive 6502	5.2	Do veterans receive an explanation regarding "Directory Opt-Out" and how it affects them?	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- Privacy Checklist**

Reference to VA Policy	Document Section	Checklist Item / Question	Comments
VA Directive 6502	5.3	Does your facility have a process for monitoring whether veterans are asked their preference for the facility directory? (Examples: calling facility to see if you can get information on someone who has opted out; monitoring intake processes to see if opt-out options are provided, etc.)	
VA Directive 6502	5.4	When veterans are admitted (from Admissions/Intake directly) are they asked for their preference regarding participation in the facility directory?	
VA Directive 6502	5.5	When veterans are admitted (from Clinic/Emergency /Ward directly) are they asked for their preference regarding participation in the facility directory?	
VA Directive 6502	5.6	When a veteran is incapacitated/ unconscious at the time of admission, does the provider use reasonable determination on behalf of the veteran concerning the directory opt-out decision?	
VA Directive 6502	5.7	Is historical data from the previous visit (if applicable) used to decide the directory preference of the veteran if they are incapacitated/unconscious at the time they are admitted?	
VA Directive 6502	5.8	Does the clinical provider document their decision about the facility directory (on behalf of the veteran), if they used reasonable determination at the time an incapacitated/unconscious veteran is admitted?	
VA Directive 6502	6.1	Are patients Confidential Communication preference information entered upon request?	
VA Directive 6502	6.2	If a patient has requested a Confidential Communication preference, is it used as requested?	
VA Directive 6502	7.1	Who monitors researcher's use of information for studies?	
VA Directive 6502	7.2	Does the Institutional Review Board (IRB) grant a "waiver of authorization" for any research study that does not require or obtain a signed authorization at your facility?	
VA Directive 6502	7.3	Do all non-VHA researchers/research assistants who participate in VHA research project have a "Without Compensation" (WOC) appointment?	
VA Directive 6502	7.4	Do researchers base their authorization form signed by the research subject (may be included in the informed consent) on recommended VHA language provided by the VHA Office of Research and Development (ORD)?	
VA Directive 6502	7.5	Are research compliance monitors (individuals from research sponsors) trained on VHA Privacy Policy before they access patient information?	
VA Directive 6502	7.6	Do research subjects authorize the release of information to researchers and compliance monitors if an IRB waiver is not provided?	
VA Directive 6502	7.7	Are VHA researchers, including WOCs, taking IIHI from your facility to offsite locations?	
VA Directive 6502	7.8	Are VHA researchers, including WOCs, taking de-identified data from your facility to offsite locations?	
VA Directive 6502	7.9	Does the research compliance officer review the process of proposed research?	
VA Directive 6502	7.1	Does your facility have a research compliance process in place that ensures privacy compliance?	
VA Directive 6502	8.1	Does your facility have a mechanism in place to ensure and accounting of disclosures is created for the following types of records:	
VA Directive 6502	8.2	Is your facility capturing an accounting of disclosures for the following?	
VA Directive 6502	8.3	Is the current version of VA form 10-5345 used within the facility?	
VA Directive 6502	8.4	Is the current version of VA form 10-5345a used within the facility?	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- Privacy Checklist**

Reference to VA Policy	Document Section	Checklist Item / Question	Comments
VA Directive 6502	8.5	Are members of the workforce ensuring all authorization forms received by the facility are in compliance with VHA Handbook 1605.1 Para. 14 before discussing IIHI?	
VA Directive 6502	8.6	What is your average processing time for an ROI request?	
VA Directive 6502	8.7	Is the current version of ROI Manager Record Management Software used in your facility's Release of Information Department?	
VA Directive 6502	8.8	Are you using the current ROI Manager Record Management Software in other areas? (e.g., Credentialing & Privileging, Human Resources, VA Police, Infection Control)	
VA Directive 6502	8.9	If you are not using the current version of the release of information, Records Manager Software in other areas, what is your alternate process for auditing/tracking disclosures? (e.g., integrated billing)	
VA Directive 6502	8.1	Do members of the workforce know when an accounting of disclosures is required?	
VA Directive 6502	8.11	Is IIHI only disclosed from the facility with an authorization or other legal authority?	
VA Directive 6502	9.1	Has your facility identified a Privacy Officer?	
VA Directive 6502	9.2	If yes, What is the name of your Privacy Officer?	
VA Directive 6502	9.3	Has your facility taken steps to introduce the Privacy Officer to the workforce?	
VA Directive 6502	9.4	How much of the Privacy Officer's time is devoted to Privacy?	
VA Directive 6502	9.5	Has the facility assigned an alternate Privacy Officer?	
VA Directive 6502	9.6	Based on the above answers, what are the names of the alternate Privacy Officer(s)?	
VA Directive 6502	9.7	Is there a Privacy Steering Committee or Privacy-focused workgroup?	
VA Directive 6502	10.1	Have all members of the workforce been trained on VHA Privacy Policies?	
VA Directive 6502	10.2	Are all new members of the workforce trained within 30 days of their hire?	
VA Directive 6502	10.3	Can your facility certify (with documentation) that all members of the workforce have been trained on Privacy Policies within the last 12 months?	
VA Directive 6502	10.4	Is VHA Privacy Policy training documented in ways that your facility is able to determine which employees have taken the training and which ones have not?	
VA Directive 6502	10.5	What method of training tracking does your facility use?	
VA Directive 6502	10.6	What indicator does your facility use to track Privacy Policy training?	
VA Directive 6502	11.1	Is there a local policy at your facility for managing the privacy complaint process?	
VA Directive 6502	11.2	Has your facility received any Privacy complaints from members of the work-force within the last year?	
VA Directive 6502	11.3	If the answer to 11.2 is "Yes", how were the Privacy complaints received (all that apply)	
VA Directive 6502	11.4	Has your facility received any Privacy complaints from veterans or members of the public within the last year?	
VA Directive 6502	11.5	If the answer to 11.4 is "Yes", how were the Privacy complaints received (all that apply)	
VA Directive 6502	11.6	Do you follow the VA/VHA standardized process for reporting Privacy complaints?	
VA Directive 6502	11.7	Your process for reporting Privacy complaints is:	
VA Directive 6502	11.8	Your facility receives complaints from:	
VA Directive 6502	11.9	Who in your facility is designated to assess Privacy complaints?	
VA Directive 6502	11.1	How are local records of Privacy complaints maintained at your facility?	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- Privacy Checklist**

<b>Reference to VA Policy</b>	<b>Document Section</b>	<b>Checklist Item / Question</b>	<b>Comments</b>
VA Directive 6502	11.11	Are Privacy complaint records at your facility retrieved by complainant's name and/or social security number?	
VA Directive 6502	11.12	If you answered "Yes" to question 11.11, under what Privacy Act System Of Records (SOR) are you maintaining the records?	
VA Directive 6502	11.13	Who does the Privacy Officer advise or consult with when a privacy complaint is lodged (as appropriate)?	
VA Directive 6502	11.14	Which members of the workforce know the process to be followed in the event of a privacy complaint?	
VA Directive 6502	11.15	Do all members of the workforce know whom to contact in the facility with privacy complaints?	
VA Directive 6502	11.16	Privacy investigations/complaints are initiated within:	
VA Directive 6502	11.17	How much time (in documented policy) has your facility established for replying to privacy complaints?	
VA Directive 6502	11.18	Privacy complaints are logged into the Privacy Violation Tracking System (PVTS) within how many days after you receive a complaint?	
VA Directive 6502	11.19	Who has access to the Privacy Violation Tracking System (PVTS) in your facility?	
VA Directive 6502	12.1	Which personnel have applicable members of the workforce been informed should be contacted in identifying business associates?	
VA Directive 6502	12.2	Are people who are not members of the VHA workforce given access to IIHI? (e.g., DoD, Accrediting Bodies)	
VA Directive 6502	12.3	If you answered "Yes" to question 12.2, are Business Associate Agreements in place, if required?	
VA Directive 6502	12.4	Has your facility identified all business associates with whom it shares IIHI for the following?	
VA Directive 6502	12.5	Do you have a fully executed business associate agreement with all business associates?	
VA Directive 6502	12.6	Do all business associate agreements authorize termination of the relationship by VHA (if VHA determines that the business associate has violated a material term of the business associate agreement)?	
VA Directive 6502	12.7	Do all business associates provide an accounting of disclosure upon request?	
VA Directive 6502	12.8	Does your facility verify all of your business associates maintain an accounting of their disclosures?	
VA Directive 6502	12.9	Do all business associate agreements require the business associate to implement safeguards consistent with the HIPAA Privacy and Security Rule requirements to protect the confidentiality, integrity and availability of the electronic PHI that it creates, receives, maintains or transmits on behalf of the facility?	
VA Directive 6502	13.1	Have local facility privacy policies and procedures been developed that comply with VHA Directive 1605 and Handbooks 1605.1 and 1605.2?	
VA Directive 6502	13.2	Do written policies and procedures regarding privacy include:	
VA Directive 6502	13.3	Are local policies and procedures at your facility reviewed or modified on a periodic basis to conform to changes in privacy legislation and regulation and VA and VHA policy changes?	
VA Directive 6502	13.4	What percentage of your staff has been assigned a Functional Category in accordance with VHA Handbook 1605.2 – Minimum Necessary Standard for Protected Health Information?	
VA Directive 6502	14.1	Does your facility have a documented and implemented Facility Directory Opt-Out Policy and Procedure?	
VA Directive 6502	15.1	Does your facility have a documented and implemented Confidential Communications Policy and Procedure?	
VA Directive 6502	16.1	Does your facility have a documented and implemented Right of Access Policy and Procedure?	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- Privacy Checklist**

Reference to VA Policy	Document Section	Checklist Item / Question	Comments
VA Directive 6502	17a	Does your facility have a documented and implemented Release of Information Policy and Procedure addressing releases of information within VHA organizations and with VA?	
VA Directive 6502	17b	Does your facility have a documented and implemented Release of Information Policy and Procedure addressing releases of information outside of VHA?	
VA Directive 6502	18.1	Does your facility have a documented and implemented Amendment of Records Policy and Procedure	
VA Directive 6502	19.1	Does your facility have a documented and implemented Accounting of Disclosure Policy and Procedure?	
VA Directive 6502	20.1	Does your facility have a documented and implemented Freedom of Information Act Policy and Procedure?	
VA Directive 6502	21.1	Does your facility have a documented and implemented Privacy Complaint(s) Policy and Procedure?	
VA Directive 6502	22.1	Does your facility have a documented and implemented Researchers Use of Information Policy and Procedure?	
VA Directive 6502	23.1	Does your facility have a documented and implemented Minimizing Incidental Disclosures or a Reasonable Safeguards Policy and Procedure?	
VA Directive 6502	24.1	Does your facility have a documented and implemented Right to Request Restriction Policy and Procedure?	
VA Directive 6502	25.1	Does your facility have a documented and implemented Authorization Requirements Policy and Procedure?	
VA Directive 6502	26.1	Does your facility have a documented and implemented VHA Privacy Policy Training Policy and Procedure?	
VA Directive 6502	27.1	Does your facility have a documented and implemented Business Associate Agreement(s) Policy and Procedure?	
VA Directive 6502	28.1	Does your facility have a documented and implemented Notice of Privacy Practices Policy and Procedure?	
VA Directive 6502	29.1	Does your facility have a documented and implemented Auditory Practices Policy and Procedure?	
VA Directive 6502	30.1	Does your facility have a documented and implemented Disclosures Via Email or Fax Policy and Procedure?	
VA Directive 6502	31.1	Does your facility have a documented and implemented Destruction of Data Policy and Procedure?	
OMB M-06-16, Action Item 1.1		Ensure the security categorization explicitly identifies PII data remotely accessible or physically removed.	
OMB M-06-16, Action Item 1.2	RA-4	Ensure the risk assessment accurately depicts the risks associated with remote access and physical removal of PII data.	
OMB M-06-16, Action Items 3.2, 4.3, 4.4	PL-4	If policy allows PII data to be stored or downloaded to a remote site, ensure a system applicable rules of behavior policy exists which requires PII data to be stored in an encrypted form at all times.  If policy allows PII to be remotely accessed only if not stored locally, ensure a system applicable rules of behavior policy exists.	
OMB M-06-16, Action Item 1.1	PL-5	Ensure the PIA identifies PII data, how it is protected when access remotely or physically removed, and states the potential impact on privacy if the data were lost, corrupted, accessed by an unauthorized individual, etc.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- Privacy Checklist**

Reference to VA Policy	Document Section	Checklist Item / Question	Comments
OMB M-06-16, Action Items 2.1, 2.2, 2.3	MP-1	<p>Ensure organizational policy addresses the information protection needs associated with PII that is accessed remotely or physically removed.</p> <p>If PII is physically removed:            a) Does the policy explicitly identify the rules for determining whether physical removal is allowed?            b) For PII that can be removed, does the policy require the information be encrypted and that appropriate procedures, training, and accountability measures are in place to ensure that remote use of this encrypted information does not result in bypassing the protections provided by the encryption?</p> <p>When remote access of PII is allowed, does the policy identify the rules for determining whether download and remote storage of the information is allowed (e.g. the policy could permit remote access to a database, but prohibit downloading and local storage of that database)?</p> <p>Based on the results of the above questions, the organizational policy should be revised or developed to fully address the above questions.</p>	
OMB M-06-16, Action Item 3.1	MP-5	<p>If PII data is transported and/or stored at a remote site, provide details on PII data encryption prior to transport (e.g. encryption of PII data using 128-bit AES encryption onto a DVD-R disc prior to transport).</p>	
OMB M-06-16, Action Items 2.1, 2.2, 2.3	AT-1	<p>Ensure organizational policy addresses the information protection needs associated with PII that is accessed remotely or physically removed.</p> <p>For PII that can be removed, does the policy require appropriate procedures and training are in place to ensure that remote use of this encrypted information does not result in bypassing the protections provided by the encryption?</p> <p>If PII is accessed remotely, does the policy identify the rules for determining whether download and remote storage of the information is allowed (e.g. the policy could permit remote access to a database, but prohibit downloading and local storage of that database)?</p> <p>Based on the results of the above questions, the organizational policy should be revised or developed to fully address the above questions.</p>	
OMB M-06-16, Action Item 4.4	AT-2	<p>If policy allows PII to be remotely accessed only if not stored locally, ensure proper awareness materials are distributed.</p>	
OMB M-06-16, Action Items 2.1, 2.2, 2.3	IA-1	<p>Ensure organizational policy addresses the information protection needs associated with PII that is accessed remotely or physically removed.</p>	
OMB M-06-16, Action Item 4.1	IA-5	<p>If policy allows PII data be accessed remotely from remote components of the system to an internal agency network, ensure the required VPN connection uses agency-controlled certificates or hardware tokens issued directly to each authorized user.</p>	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- Privacy Checklist**

Reference to VA Policy	Document Section	Checklist Item / Question	Comments
OMB M-06-16, Action Items 2.1, 2.2, 2.3	AC-1	<p>Ensure organizational policy addresses the information protection needs associated with PII that is accessed remotely or physically removed.</p> <p>If PII is accessed remotely:</p> <p>a) Does the policy explicitly identify the rules for determining whether remote access is allowed?</p> <p>b) When remote access is allowed, does the policy require that this access be accomplished via a virtual private network (VPN) connection established using agency-issued authentication certificate(s) or hardware token?</p> <p>c) When remote access is allowed, does the policy identify the rules for determining whether download and remote storage of the information is allowed (e.g. the policy could permit remote access to a database, but prohibit downloading and local storage of that database)?</p> <p>Based on the results of the above questions, the organizational policy should be revised or developed to fully address the above questions.</p>	
OMB M-06-16, Action Items 4.2, 4.4	AC-3	<p>If policy allows PII data be downloaded to a remote location, ensure access is limited to permitted information only.</p> <p>If policy allows PII to be remotely accessed only if not stored locally, ensure access is limited to permitted information only.</p>	
OMB M-06-16, Action Items 4.2, 4.4	AC-4	<p>If policy allows PII data be downloaded to a remote location, ensure controls are in place to permit only allowed information to be transmitted across the remote interface.</p> <p>If policy allows PII to be remotely accessed only if not stored locally, ensure controls are in place to permit only allowed information to be transmitted across the remote interface.</p>	
OMB M-06-16, Action Items 4.2, 4.4	AC-6	<p>If PII data is accessed remotely, ensure controls are in place to enforce the most restrictive rights to the information while still allowing the individual to perform their job duties.</p> <p>If policy allows PII to be remotely accessed only if not stored locally, ensure controls are in place to enforce the most restrictive rights to the information while still allowing the individual to perform their job duties.</p>	
OMB M-06-16, Action Items 4.2, 4.4	AC-13	<p>If policy allows PII data be downloaded to a remote location, ensure activity logs are reviewed to maintain accountability for actions taken across remote interfaces.</p> <p>If policy allows PII to be remotely accessed only if not stored locally, ensure activity logs are reviewed to maintain accountability for actions taken across remote interfaces.</p>	
OMB M-06-16, Action Items 4.1, 4.4	AC-17	<p>If policy allows PII data be accessed remotely from remote components of the system to an internal agency network, ensure a VPN connection is required for each authorized user.</p> <p>If policy allows PII to be remotely accessed only if not stored locally, ensure a VPN connection is required for each authorized user.</p>	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- Privacy Checklist**

Reference to VA Policy	Document Section	Checklist Item / Question	Comments
OMB M-06-16, Action Items 2.1, 2.2, 2.3	AU-1	<p>Ensure organizational policy addresses the information protection needs associated with PII that is accessed remotely or physically removed.</p> <p>For PII that can be removed, does the policy require the information be encrypted and that appropriate accountability measures are in place to ensure that remote use of this encrypted information does not result in bypassing the protections provided by the encryption?</p> <p>Based on the results of the above questions, the organizational policy should be revised or developed to fully address the above questions.</p>	
OMB M-06-16, Action Items 4.2, 4.4	AU-2	<p>If policy allows PII data be downloaded to a remote location, ensure remote audit events are recorded to maintain accountability for actions taken across remote interfaces.</p> <p>If policy allows PII to be remotely accessed only if not stored locally, ensure remote audit events are recorded to maintain accountability for actions taken.</p>	
OMB M-06-16, Action Items 4.2, 4.4	AU-6	<p>If policy allows PII data be downloaded to a remote location, ensure audit logs are reviewed to maintain accountability for actions taken across remote interfaces.</p> <p>If policy allows PII to be remotely accessed only if not stored locally, ensure audit logs are reviewed to maintain accountability for actions taken.</p>	
OMB M-06-16, Action Items 2.1, 2.2, 2.3	SC-1	<p>Ensure organizational policy addresses the information protection needs associated with PII that is accessed remotely or physically removed.</p> <p>If PII is accessed remotely:</p> <p>a) Does the policy explicitly identify the rules for determining whether remote access is allowed?</p> <p>b) When remote access is allowed, does the policy require that this access be accomplished via a virtual private network (VPN) connection established using agency-issued authentication certificate(s) or hardware token?</p> <p>Based on the results of the above questions, the organizational policy should be revised or developed to fully address the above questions.</p>	
OMB M-06-16, Action Items 3.2, 4.3, 4.4	SC-4	<p>If policy allows PII data to be stored or downloaded to a remote site, ensure personnel receive training notifying them of the PII data encryption requirement.</p> <p>If policy allows PII to be remotely accessed only if not stored locally, ensure personnel receive training notifying them of the PII data handling policy.</p>	
OMB M-06-16, Action Items 3.1, 3.2, 4.3	SC-13	<p>If policy allows PII data to be stored or downloaded to a remote site, provide details on the cryptography used to encrypt the PII data.</p>	
VA Directive 6502	3.f	<p>VA personnel, contractors, and authorized users shall report all actual or suspected breaches of privacy in a timely and complete manner to agents designated by the Privacy Service. VA shall resolve all such issues of breach of privacy according to applicable law and in a timely fashion.</p>	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- Privacy Checklist**

Reference to VA Policy	Document Section	Checklist Item / Question	Comments
VA Directive 6502	3.g	The physical input and output products of VA information systems that contain privacy-protected data, such as disks, paper, and compact disks (CD), shall be protected against misuse and unauthorized access, disclosure, modification, or destruction.	
VA Directive 6502	3.h	Security plans shall be developed and security controls implemented on the networks that transmit and store privacy-protected data. These controls shall be implemented, as required by law, to protect the security and privacy of the operating system, applications software, and data in VA information systems from accidental or malicious alteration or destruction, and to provide assurances to the user of the quality and integrity of VA maintained privacy-protected data.	
VHA Handbook 1605.1	3.a.(5)	Information about individuals that is retrieved by a personal identifier may not be collected or maintained until proper notifications are given to Congress and the Office of Management and Budget (OMB), and until published in the Federal Register as required by the Privacy Act.	
VHA Handbook 1605.1	3.a.(6)	Each Veterans Integrated Service Network (VISN) and VA medical center or VA Health Care System must designate a Privacy Officer and a FOIA Officer (see 38 CFR 1.556). One employee can serve as both the Privacy Officer and FOIA Officer.	
VHA Handbook 1605.1	3.b.(2)	Sharing of individually-identifiable information within VHA, or between VHA and other VA components, or VHA and VA Contractors must be conditioned on the completion of a data use form, which specifies the conditions for the provision of data. NOTE: For VA research see subparagraph 3b(3). A sample suggested data use form is referenced in Appendix E, VHA Data Use Form. Violation of the terms of the agreement will result in termination of the party's right to future access of such data and may require additional legal action, including referral for criminal prosecution, or in the case of VA employees, disciplinary or other adverse action. Consequently, legal counsel needs to be consulted upon learning of any violation of this agreement.	
VHA Handbook 1605.1	3.c.(1)	Individually-identifiable information is to be disclosed to requestors with the understanding that it is confidential information that needs to be handled with appropriate sensitivity.	
VHA Handbook 1605.1	3.c.(3)	Information from VHA records can only be disclosed or released with the prior signed authorization of the individual or other legal authority as outlined in this Handbook. All disclosures must be covered by or listed in the Information Bulletin (IB) 10-163, VA Notice of Privacy Practices.	
VHA Handbook 1605.1	3.c.(5)	For sharing of individually-identifiable information with other Federal entities for auditing and oversight, as authorized by law and this Handbook, VHA needs to request the completion of a data use form which specifies the conditions for the provision of data (see App. For example, for audits performed by the General Accounting Office (GAO), a data use agreement in this situation is not required, but discretionary.	
VHA Handbook 1605.1	3.d.(1)	VHA, including each health care facility, must ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of individually-identifiable information and records, including protected health information (PHI) and records, and to protect against any anticipated threats or hazards to their security or integrity which would result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- Privacy Checklist**

Reference to VA Policy	Document Section	Checklist Item / Question	Comments
VHA Handbook 1605.1	3.d.(2)	Each health care facility must develop clear and explicit policies governing employees' auditory privacy when discussing sensitive patient care issues. Employees need to be conscious of when and where it is appropriate to discuss issues involving an individual's identifiable health information.	
VHA Handbook 1605.1	37.a.(2)	Other than the two exceptions below, does the VA health care facility participate in computer matching programs with other Federal agencies or non-Federal agencies as a "recipient agency" or a "source agency"?: (a) Approved by the VA health care facility Director, VHA Privacy Officer, appropriate VA Central Office staff, and the VA Data Integrity Board; and (b) Conducted in compliance with the Privacy Act (as amended by the Computer Matching Act), the OMB guidelines (65 FR 77677, December 12, 2000) and applicable Department guidance (VA Handbook 6300.7).	
VHA Handbook 1605.1	36.(b)	Information concerning an individual will not be collected or maintained in such a manner that information is retrieved by an individual identifier, unless a system notice is first published in the Federal Register.	
VA Directive 6300		VA will maintain a Data Integrity Board (DIB) to ensure that computer matching agreements comply with the requirements of the Computer Matching and Privacy Protection Act of 1988 and the Office of Management and Budget (OMB)	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- Research Special Emphasis**

Reference to VA Policy	Document Section	Checklist Item / Question	Comment
VHA Handbook 1200.5 §7.a(7)	A.1	Adequate provisions are in place to protect the privacy of subjects and to maintain the confidentiality of individually-identifiable data.	
VHA Handbook 1200.5 §7.d(12); VHA Handbook 1605.1 §13; VA Directive 6504 §2s	A.2	Institutional Review Board (IRB) has established written procedures that accurately reflect the requirements for reporting to the Privacy Officer any unauthorized use, loss, or disclosure of individually-identifiable patient information.	
VHA Handbook 1200.5 §7.d(13)	A.3	IRB has established written procedures that accurately reflect the requirements for reporting violations of VA information security requirements to the appropriate VHA Information Security Officer.	
VHA Handbook 1200.5 §13b.	A.4	Obtaining and using medical, technical, and administrative records from other VA facilities or VA databases (national, regional, or subject specific) for R&D purposes are in compliance with all VHA regulations and with the Standards for Privacy of Individually-Identifiable Health Information (45 CFR Parts 160 and 164).	
VHA Handbook 1200.5 §13b.	A.5	Obtaining and disclosing individually-identifiable patient records are in compliance with all applicable confidentiality statutes and regulations including those discussed in subparagraph 7a(7) of VHA Handbook 1200.5.	
VHA Handbook 1200.5 §13c.	A.6	Persons not employed by VA are given access to medical and other VA records for R&D purposes <u>only</u> within the legal restrictions imposed by such laws as the Privacy Act of 1974; 38 USC §5701, §5705, §7332; and VHA Handbook 1605.1 §13b (also see E3, E4, & E6).	
VHA Handbook 1200.5 §13c.	A.7	Access to medical and other VA records for R&D purposes by persons not employed by VA is approved by CRADO (also see E3).	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- Research Special Emphasis**

Reference to VA Policy	Document Section	Checklist Item / Question	Comment
VHA Handbook 1200.5, Appendix B, 1b.	A.8	The IRB expedited review process is not used when identification of the subjects and/or their responses would reasonably place them at risk of criminal or civil liability; or be damaging to the subject's financial standing, employability, insurability, and/or reputation; or be stigmatizing, unless reasonable and appropriate protections are implemented so that risks related to invasion of privacy and breach of confidentiality are minimal.	
VHA Handbook 1200.5, Appendix C, 2.a(7)	A.9	Informed consent contains a description of any reasonably foreseeable risks or discomforts to the subject including for example, privacy risks (legal, employment, and social).	
VHA Handbook 1200.5, Appendix E, 1; VHA Handbook 1605.1 §13	A.10	IRB documents the findings on which it based its decision for granting a waiver or alteration of the HIPAA Authorization requirement.	
Memo from DUSHOM & CRADO on 06/12/06 <i>"Research Responsibilities for Protecting Sensitive Information"</i>	B.1	Researchers are familiar with and abide by existing policies, procedures and directives regarding the protection of human subjects in research and the use and disclosure of individually-identifiable information as outlined in VHA Handbook 1200.5, VA IT Directive 06-2, VHA Handbook 1605.1, and VA Directive 6504 (also see D & E).	
Memo from DUSHOM & CRADO on 06/12/06 <i>"Research Responsibilities for Protecting Sensitive Information"</i>	B.2	All removable or transferable storage media (flash drives, CD ROMs, laptops, etc.) are reviewed to remove or secure sensitive information (also see D8, D20, D23, & D25).	
VA IT Directive 06-2; "Safeguarding Confidential and Privacy Act-Protected Data at Alternative Work Locations" (06/06/06)	B.3	Employees authorized to remove confidential and Privacy Act-protected data from VA take all relevant precautions to safeguard that data until it is returned (also see D8-D27).	
VA IT Directive 06-2; "Safeguarding Confidential and Privacy Act-Protected Data at Alternative Work Locations" (06/06/06)	B.4	Employees authorized to remove electronic data consult with their supervisors and Information Security Officers (ISOs) to ensure the data is properly encrypted and password-protected in accordance with VA policies (also see D1, D4, D19, D20, & D24).	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- Research Special Emphasis**

Reference to VA Policy	Document Section	Checklist Item / Question	Comment
VA IT Directive 06-2	B.5	Employees who remove confidential and Privacy Act-protected data from VA premises have written authorization to do so (also see D24).	
<i>"Safeguarding Confidential and Privacy Act-Protected Data at Alternative Work Locations" (06/06/06)</i>	B.6		
VA IT Directive 06-2; <i>"Safeguarding Confidential and Privacy Act-Protected Data at Alternative Work Locations" (06/06/06)</i>	B.7	Employees handle confidential and Privacy Act-protected data as instructed by VA policies (also see D, &E).	
VA IT Directive 06-2; <i>"Safeguarding Confidential and Privacy Act-Protected Data at Alternative Work Locations" (06/06/06)</i>	B.8	Employees report the loss of confidential or Privacy-Act protected data immediately to the facility ISO, Privacy Officer, and his/her supervisor (also see D22).	
PDUSH Memo on 06/27/06 <i>"Cyber Security and Privacy"</i>	B.9	All employees have taken the mandatory annual training for VA Cyber Security Awareness and VHA Privacy Policy.	
PDUSH Memo on 07/10/06 <i>"Researcher Contacts with Veterans"</i>	B.10	Contact with veterans is limited to those clinically essential or as outlined in IRB approved protocols. Contacts do not solicit sensitive information (e.g., SSNs).	
PDUSH Memo on 07/10/06 <i>"Researcher Contacts with Veterans"</i>	B.11	During the recruitment process, researchers make initial contacts with veterans in person and/or by letter prior to any telephone contact, and provide a telephone number or other means that veterans can use to verify the validity of the study.	
PDUSH Memo on 07/10/06 <i>"Researcher Contacts with Veterans"</i>	B.12	Informed consent documents used after July 10, 2006 include information about where and how a veteran could verify the validity of a study and authorized contacts.	
PDUSH Memo on 07/10/06 <i>"Researcher Contacts with Veterans"</i>	B.13	After recruitment and during follow-up phase, researchers begin calls by referring to previous contacts and the information provided on the informed consent document.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- Research Special Emphasis**

Reference to VA Policy	Document Section	Checklist Item / Question	Comment
Interim SOP, Section 1 "Notifying Veterans of Incidents Involving Compromised Personal Information" (Interim Standard Operating Procedures (SOP), Office of Information & Technology, November 22, 2006)	C.1	The substance of the notice to the veteran about an incident involving personal information is reduced to a stand-alone document and written in clear, concise, and easy-to-understand language, capable of individual distribution and/or posting on VA's website and other information sites.	
Interim SOP, Section 1 "Notifying Veterans of Incidents Involving Compromised Personal Information" (Interim Standard Operating Procedures (SOP), Office of Information & Technology, November 22, 2006)	C.2	Written notifications to veterans include all elements listed in Section 1 of the SOP.	
Interim SOP, Section 2 "Notifying Veterans of Incidents Involving Compromised Personal Information" (Interim Standard Operating Procedures (SOP), Office of Information & Technology, November 22, 2006)	C.3	All notifications use only the templates attached to the SOP.	
Interim SOP, Section 2 "Notifying Veterans of Incidents Involving Compromised Personal Information" (Interim Standard Operating Procedures (SOP), Office of Information & Technology, November 22, 2006)	C.4	All notification letters (Initial Incident Notification, Credit Protection Notification, and Deceased Veteran Notification) are reviewed by facility incident response team, facility Office of Public and Intergovernmental Affairs and Regional Counsel, as well as the VISN and National Level Incident response team, if appropriate.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- Research Special Emphasis**

Reference to VA Policy	Document Section	Checklist Item / Question	Comment
Interim SOP, Section 2 "Notifying Veterans of Incidents Involving Compromised Personal Information" (Interim Standard Operating Procedures (SOP), Office of Information & Technology, November 22, 2006)	C.5	VISN Director and VACO-assigned VISN 10N Health System Specialist or designee are notified after the Notification Letters receive local clearance and prior to mailing to veterans. Institutional policies specify who is responsible for notifying the VISN 10N Health System Specialist or designee.	
Interim SOP, Section 2 "Notifying Veterans of Incidents Involving Compromised Personal Information" (Interim Standard Operating Procedures (SOP), Office of Information & Technology, November 22, 2006)	C.6	No Notification Letters are mailed to the veterans without first obtaining 10N and VHA Privacy Office concurrence.	
Interim SOP, Section 2 "Notifying Veterans of Incidents Involving Compromised Personal Information" (Interim Standard Operating Procedures (SOP), Office of Information & Technology, November 22, 2006)	C.7	Notification Letters regarding deceased veterans are sent to veteran's next-of-kin, and information in the letter is tracked using the spreadsheet in Attachment D of the SOP.	
Interim SOP, Section 3 "Notifying Veterans of Incidents Involving Compromised Personal Information" (Interim Standard Operating Procedures (SOP), Office of Information & Technology, November 22, 2006)	C.8	Determination that credit protection services should be offered is made according to Section 3 of the SOP.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- Research Special Emphasis**

<b>Reference to VA Policy</b>	<b>Document Section</b>	<b>Checklist Item / Question</b>	<b>Comment</b>
Interim SOP, Section 4 "Notifying Veterans of Incidents Involving Compromised Personal Information" (Interim Standard Operating Procedures (SOP), Office of Information & Technology, November 22, 2006)	C.9	Facility maintains a record of how Promotional Codes for credit protection are dispersed, and ensures that information listed in Section 4 of the SOP is available when requested by VACO.	
Interim SOP, Section 5 "Notifying Veterans of Incidents Involving Compromised Personal Information" (Interim Standard Operating Procedures (SOP), Office of Information & Technology, November 22, 2006)	C.10	Facility provides an 800-number or local call line to impacted veterans for questions, and implements all steps described in Section 5 of the SOP to ensure the lines are adequately and appropriately staffed.	
VA Directive 6504 §2a; §3c	D.1	Employees obtain their supervisors' approval to transport, transmit, access, and use VA data outside VA facilities.	
VA Directive 6504 §2b	D.2	Only VA-owned Government Furnished Equipment (VAGFE), including laptops and handheld computers, are used when accessing the VA intranet remotely, and all required security software is installed and updated to connect to the VA Virtual Private Network (VPN) in such a way that grants full VA access.	
VA Directive 6504 §2b	D.3	Access to the VA Intranet using non-VA owned Other Equipment (OE) is provided via approved VA VPN access protocols, which offer access to a limited set of VA applications and services.	
VA Directive 6504 §2c; §3c	D.4	Employees obtain supervisory approval for remote access to the VA Intranet.	
VA Directive 6504 §2c(1); §3d	D.5	ISO disables the remote access account if it is not used for a period of 90 days and removes the account if it is not used for 6 months.	
VA Directive 6504 §2c(2)	D.6	Upon termination of required access privileges, supervisors confirm and notify the ISO that the employee has returned all VAGFE related to remote access.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- Research Special Emphasis**

Reference to VA Policy	Document Section	Checklist Item / Question	Comment
VA Directive 6504 §2d	D.7	Only VA personnel access VA-owned equipment used to process VA information or access VA processing services.	
VA Directive 6504 §2e; §3c	D.8	Employees use only computers and electronic storage media configured to conform to all VA security and configuration policies to store, transport, transmit, use and access VA Protected Information (VAPI).	
VA Directive 6504 §2e(1); §2e(2)	D.9	Use of VAGFE and OE meets all requirements listed in VA Directive 6504 §2e.	
VA Directive 6504 §2f(1)	D.10	VAGFE and OE that contain VAPI are equipped with, and use, a VA-approved antivirus (AV) software and a personal (“host-based”) firewall that is configured with a VA-approved configuration.	
VA Directive 6504 §2f(2)	D.11	In the event that the computer/device connecting remotely is simultaneously attached to a second network (such as an in-home LAN), the secondary network computers/devices are provided with similar AV and host-based/personal firewall protection.	
VA Directive 6504 §2f(3)	D.12	All VAGFE devices attempting to access the VA intranet remotely via the One-VA VPN client have the AV and Host-based Intrusion Prevention System (HIPS) software installed and current, including all critical updates and patches, in order to be granted access to the VA intranet.	
VA Directive 6504 §2g; §3c	D.13	Employees using non-VA OE devices to access the VA intranet remotely comply with the policy set forth in <i>“Anti-Virus/Firewall accepted for use on non-government owned equipment attached to the One-VA VPN”</i> (May 5, 2005)	
VA Directive 6504 §2i; §3c	D.14	Employees using a VAGFE or non-VA OE to connect to the internet outside the regular work site ensure that the computer is protected by a firewall.	
VA Directive 6504 §2k; §3c	D.15	Employees follow procedures described in VA Directive 6504 §2k when handling viral or malicious code infection.	
VA Directive 6504 §2l; §3c	D.16	Employees do not simultaneously connect to VA and one or more non-VA networks while using VAGFE.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- Research Special Emphasis**

Reference to VA Policy	Document Section	Checklist Item / Question	Comment
VA Directive 6504 §2n	D.17	Wireless routers and access points, even if not used at the enclave perimeter, are configured in accordance with the “VA Wireless and Handheld Device Security Guideline” (Version 3.2, August 15, 2005)	
VA Directive 6504 §2p(1)	D.18	VAPI is not transmitted by remote access unless VA-approved protection mechanisms are used.	
VA Directive 6504 §2p(2)	D.19	Passwords or other authentication information are not stored on remote systems unless encrypted.	
VA Directive 6504 §2q	D.20	Approved encryption software is used when employees use VAGFE or non-VA OE in a mobile environment [e.g. laptop or Personal Digital Assistant (PDA) carried out of a VA office or a PC in an alternative work site] and VAPI is stored on the computer, file or electronic storage media.	
VA Directive 6504 §2r	D.21	Employees make redundant copies (“backups”) of essential business data and software on remote or mobile computers at regular intervals, and store multiple sets of backup data in protected locations other than the location of the device containing the data.	
VA Directive 6504 §2s; §3c	D.22	Employees immediately report incidents involving theft, loss or compromise of any VAGFE or non-VA OE device used to transport, access or store VA information, or any VAPI to his or her supervisor and the local ISO.	
VA Directive 6504 §2t	D.23	When no longer needed, VA information classified as VA sensitive is destroyed by a method rendering it unreadable, undecipherable, and irretrievable as prescribed in the most current version of “Fixed Media Sanitization” (VA Memo, April 20, 2004) and its attachment.	
VA Directive 6504 §2u(1); §3c	D.24	For all VAGFE and non-VA OE used to transmit, transport, access, process or store VA data, employees do not take equipment, information, or software off-site without authorization by supervisor.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- Research Special Emphasis**

Reference to VA Policy	Document Section	Checklist Item / Question	Comment
VA Directive 6504 §2u(3)	D.25	Portable computers that have VAPI on their storage device(s) or have software that provides access to VA private networks are secured under lock and key when not in the immediate vicinity of the responsible employee.	
VA Directive 6504 §2u(4); §3c	D.26	Employees use physical locks to secure portable computers to immovable objects when the computers must be left in a meeting room, or other semi-public area to which individuals other than the authorized employee have access.	
VA Directive 6504 §2u(6); §3c	D.27	When traveling, employees keep portable computers or storage devices in their possession, not in check-in baggage.	
VA Handbook 1605.1 §13a(2)(b)	E.1	VHA investigators obtain written authorization or a waiver of authorization requirement from IRB for using VHA individually-identifiable health information involving non-employee research subjects for research purposes.	
VA Handbook 1605.1 §13a(2)(d)	E.2	VHA investigators use the requested data only in a manner consistent with the approved research protocol for which the information was requested.	
VA Handbook 1605.1 §13b	E.3	Disclosure of individually-identifiable information to non-VHA investigators for research purposes is approved by CRADO.	
VA Handbook 1605.1 §13b(1)(a)	E.4	Written authorization is obtained for disclosing VHA individually-identifiable health information involving non-employee research subjects by a VHA investigator to non-VHA investigators for research purposes.	
VA Handbook 1605.1 §13b(1)(b)	E.5	Without prior written authorization, disclosure of individually-identifiable health information, excluding 38 USC §7332-protected information, to Federal investigators is made only when the Under Secretary for Health or designee has approved the research, and an IRB or Privacy Board has waived the authorization requirement.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- Research Special Emphasis**

Reference to VA Policy	Document Section	Checklist Item / Question	Comment
VA Handbook 1605.1 §13b(1)(c)	E.6	Without prior written authorization, disclosure of individually-identifiable health information, excluding 38 USC §7332-protected information and names and addresses of the individual subjects, to non-Federal investigators is made only when approval by the Under Secretary for Health or designee, and waiver of authorization requirement by IRB or Privacy Board are obtained.	
VA Handbook 1605.1 §13b(1)(d)	E.7	Title 38 USC §7332-protected information is disclosed without written authorization only when conditions listed in VA Handbook 1605.1 §13b(1)(d) are met.	
VA Handbook 1605.1 §13b(2)(a)	E.8	The individually-identifiable information of research subjects in their capacity as VHA employees, excluding health information, is disclosed to non-VHA Investigators for research purposes without written authorization only in accordance with the Privacy Act and applicable VA privacy policy.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- Record Management Checklist**

Checklist Item / Question	Comment
Identified Records Management Officer	
Annual specialized training for the Records Administrator, FOIA, and the PA Officer.	
Annual general program training for all employees on records management	
Shredders are available to shred sensitive documents.	
The Records Administrator and Records Managers are knowledgeable of the retention values for records to include paper, IT, and web records.	
Employee Clearance addresses record issues of those departing employees maintaining case files/official records at their respective desks/cubicles/offices.	
Records are disposed of in accordance with the Agency's records disposal policy and procedures.	
Records Officer periodically reviews the National Archives and Records Administration (NARA) ( <a href="http://www.nara.gov">www.nara.gov</a> ) to keep apprised of new records management issues and concerns.	
FOIA case files are complete, consisting of file folders with the FOIA number and a copy of the incoming request, outgoing response letters, and all file correspondence including documentation regarding consultations, copies of released records (both un-	
FOIA files are to be disposed of in accordance with the VHA Records Control Schedule (RCS) 10-1.	
Are office and file cabinets containing sensitive material locked after hours?	
Are Privacy Act records locked at all times?	
Databases that collect personal information compliant with OMB requirements, Privacy Act System Notices, and Privacy Impact Assessments?	
Controls in place to check-out, check-in files ensure that all files are returned to a controlled area before closing for the day?	
Records personnel are knowledgeable regarding what documents constitute a record such as e-mail, telephone conversation notes, meeting minutes, decision documents.	
An imaged document must be an adequate duplicate of the paper document. The imaged document must be retained for the same length of time that the paper document was authorized for retention.	
Labels on file drawers should include an accurate description of the drawer content. The label should tell the series and/or the range of records stored within.	
Drawers that contain Privacy Act information should have Privacy Act label affixed and must be properly secured with restricted access.	
Any records stored in warehouses should be inventoried and physically located together.	
Records are to be stored at the VA Records Center and Vault or at a records storage facility authorized by the NARA..	
The local Records Management Officer authorizes any storing of record material in the warehouse prior to that occurrence.	
Inactive records should be stored at the VA Records Center and Vault. Active records may be stored at a facility warehouse. Records should not be stored at a commercial warehouse unless approved by NARA.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- Record Management Checklist**

Checklist Item / Question	Comment
The Records Management Officer records inventory includes records located at warehouse or other off-site locations and where those records can be found.	
Warehouse space used to store records need to be physically segregated from the rest of the warehouse and access to this area strictly controlled.	
Smoke detectors should be placed in the area where records are stored.	
Smoke detectors and overhead sprinklers need to be installed to mitigate damage as a result of a fire. Appropriate safeguards are to be taken to prevent the premature destruction of records as a consequence of a disaster.	
Official records should be protected by closing (where possible) cabinets/flippers, etc. to shield records in the event of fire or sprinklers going off.	
Records stored in warehouses should be placed on a pallet and shrink wrapped to avoid damage in the event of water leaks.	
The records inventory should be updated annually in all offices, and should include electronic records unless a separate electronic records inventory exists. The inventory should include information on master files and backup files.	
The electronic records inventory should be updated annually.	
Locking file cabinets and/or locking fireproof cabinets used for storage of vital and sensitive records.	
Records are to be destroyed in accordance with the VHA RCS 10-1 or other appropriate record disposal manual such as the NARA General Records Schedule	
Files boxed for shipping should have sufficiently detailed box listings to include destruction dates.	
For records to be shipped to the VA Records Center, a detailed box listing is to be prepared pursuant to VA Record Center guide. For records stored at other locations, detailed box listing is to be prepared in accordance with the Agency policy.	
Appropriate measures are taken to ensure the survival of vital records (or copies of the vital records) in case of emergency or disaster.	
Vital records backups/duplicates (as well as computer system backups) should be stored at a sufficient distance to be safe and available in the event of a regional disaster.	
Records, which are being retained as a result of a court order, need to be retained until the order has been rescinded. After the order has been lifted, the records are to be destroyed in accordance with their record retention provisions.	
Walls around rooms holding Privacy Act records should be from the floor to the ceiling.	
Contract folders should be labeled and include detailed information such as date of record, identifying information like contract number, and cutoff and retention information.	

**VA Office of IT Oversight and Compliance (ITO&C)  
Compliance Assessment --- Record Management Checklist**

<b>Checklist Item / Question</b>	<b>Comment</b>
Records are to be retained in accordance with the VHA RCS 10-1 or other appropriate retention schedule such as the NARA General Records Control Schedule.	