**Department of Veterans Affairs**
**Washington, DC 20420**

**VA DIRECTIVE 6500**
**Transmittal Sheet**
**February 24, 2021**

# VA CYBERSECURITY PROGRAM

1. **REASON FOR ISSUE:** Reissues VA Directive 6500 pursuant to the authority to maintain a VA cybersecurity and privacy program to protect and defend VA information and VA Information Technology (IT) that is consistent with the VA's information privacy and security statutes, 38 United States Code (U.S.C.) §§ 5721-5728, the Federal Information Security Modernization Act (FISMA), 44 U.S.C. §§ 3551-3558, and Office of Management and Budget (OMB) Circular A-130 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53.

2. **SUMMARY OF CONTENTS/MAJOR CHANGES:**

   a. Establishes the Risk Executive Function as a component of the VA's information security governance structure (Page 7, Section 2.a.(3)(f));

   b. Establishes the Information Security Knowledge Service as the VA's centralized repository to provide cybersecurity and privacy policies, procedures, and guidance (Page 7, Section 2.a.(3)(g));

   c. Introduces and describes new Information Security Knowledge Service portal and new supporting Risk Management Framework (RMF) Technical Advisory Group (TAG) roles and responsibilities (Page 4, Section 2);

   d. Establishes the Committee on National Security Systems Instruction (CNSSI) No. 1253 as the methodology to categorize VA Information Systems (ISs), select and tailor security and privacy controls, and provide the information security control baseline for all VA Information Systems (Page 4, Section 2).

3. **RESPONSIBLE OFFICE:** Office of the Assistant Secretary for Information and Technology (OIT) (005) and Office of Information Security (OIS) (005R).

4. **RELATED HANDBOOK:** VA Handbook 6500, VA Risk Management Framework.

5. **RESCISSIONS:** VA Directive 6500, Managing Information Security Risk: VA Information Security Program, dated January 23, 2019.

**CERTIFIED BY:**

/s/
John P. Medve
Acting Assistant Secretary for
Enterprise Integration

**BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:**

/s/
Dominic A. Cussatt
Acting Assistant Secretary for Information and Technology/ Chief Information Officer

**DISTRIBUTION**: Electronic only

## TABLE OF CONTENTS

VA CYBERSECURITY PROGRAM

## 1. PURPOSE.

The purpose of the VA cybersecurity and privacy program is to set the direction for the protection and informed risk management of VA information and VA Information System (IS). This directive:

a. Reissues VA Directive 6500 to establish a VA cybersecurity and privacy program to protect and defend VA information and VA IT;

b. Establishes the Risk Executive Function as a component of the VA's information security governance structure;

c. Establishes the Information Security Program Risk Management Framework (RMF) Technical Advisory Group (TAG), which serves as the governing body for security control management and implementation, to strengthen VA's ability to rapidly deploy secure systems;

d. Establishes the Information Security Knowledge Service as VA's centralized repository to provide cybersecurity and privacy policies, procedures, and guidance;

e. Aligns VA's Information Security Program with the National Institute of Standards and Technology (NIST) Cybersecurity Framework; and

f. Designates Committee on National Security Systems Instructions (CNSSI) No. 1253 as the methodology to categorize VA Information Systems, select and tailor security and privacy controls, and provide the security control baselines for all VA Information Systems.

**2. POLICY.** VA Cybersecurity Program. VA will use this directive as well as the RMF as defined in NIST Special Publication (SP) 800-37, NIST SP 800-39, NIST SP 800-53 and as implemented by VA Handbook 6500, to manage risks to VA's information systems. VA will use Control Correlation Identifiers (CCI) level for implementation of the security and privacy controls as defined in NIST SP 800-53 and CNSSI 4009 and will follow the security control baselines in CNSSI No. 1253. This information will be located on the VA Information Security Knowledge Service.

The five core cybersecurity and privacy functions that define the VA cybersecurity and privacy program are based on the NIST Cybersecurity Framework and the Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,* issued on May 11, 2017. The core functions are: Identify, Protect, Detect, Respond, and Recover. Collectively, these five core functions enable VA to: provide mission and operational resilience under any cyber situation or condition; act collectively, consistently, and effectively in its own defense; allow VA IT to perform as designed and adequately meet operational requirements; and work securely and seamlessly among mission partners.

a. Identify Function. The Identify Function defines the foundational policies necessary to apply the Cybersecurity Framework to VA and institutionalizes VA's understanding and the processes necessary to manage cybersecurity and privacy risk to systems, assets, data, and capabilities, and identify any gaps in VA's cybersecurity and privacy practices. Outcome categories within the Identify Function are described below:

(1) Asset Management

(a) All assets (e.g., data, personnel, devices, systems, and facilities) consistent with their relative importance to VA business objectives and risk strategy must be identified and managed.

(b) All VA Information Systems must be registered in the VA System Inventory (VASI) in accordance with VA policy and as part of a security authorization in VA's Governance, Risk and Compliance tool at the Department level.

(c) VA will register all non-IT systems (e.g., physical plant systems and medical device systems) at the Department level.

(d) Information flow control policies must be developed, and approved authorization enforced for controlling the flow of information within the system and between interconnected systems.

(e) VA will meet regulatory requirements for the management of information in electronic format including Health Insurance Portability and Accountability Act (HIPAA) compliance for electronic health information.

(2) Business Environment

(a) Cybersecurity and privacy responsibilities and risk management decisions will be informed utilizing an understanding of VA's three major business environments (health, benefits, and memorial affairs).

(b) VA mission and business processes, the resulting IT processing needs, and inherent risks associated with processing electronic sensitive VA data, especially Personally Identifiable Information (PII) and electronic Protected Health Information (ePHI) must be defined and the appropriate security controls must be in accordance with FISMA, the Privacy Act, HIPAA, the Health Information Technology for Economic and Clinical Health Act (HITECH).

(c) A plan for managing financial and supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services must be developed and implemented.

(d) A critical infrastructure and key resources protection plan must be developed, documented and regularly updated to address information security and privacy issues.

(e) Critical system assets supporting essential mission and business functions must be identified to ensure additional safeguards and countermeasures can be employed and to facilitate the prioritization of organizational resources.

(f) A criticality analysis must be performed when an architecture or design is developed including the use of authoritative sources to identify critical system components and functions. Component and function criticality are assessed in terms of the impact of a component or function failure on the organizational missions supported by the system containing those components and functions.

(g) Performance is measured, assessed for effectiveness, and managed relative to contributions to mission outcomes and strategic goals and objectives in accordance with 40 U.S.C 11313 Performance and results-based management.

(h) Cybersecurity and privacy solutions must be implemented consistent with enterprise architecture principles and guidelines within the VA Architecture Framework and VA cybersecurity and privacy architectures developed or approved by the VA Chief Information Officer (CIO).

(i) Operational resilience must be implemented by requiring three conditions to be met: (i) information resources are trustworthy; (ii) missions are ready for information resources degradation or loss; and (iii) network operations have the means to prevail in the face of adverse events.

(j) Resiliency requirements to support the delivery of critical services during all operating states (e.g., under duress, under attack, during recovery, and normal operations) are defined based on the criticality of the system to enable VA to complete its mission.

(3) Governance

(a) VA will define Governance practices that include the policies, procedures, processes; guidance to manage and monitor VA's regulatory, legal, risk, environmental, and operational requirements shall be defined and to inform management of cybersecurity and privacy risks.

(b) VA will develop, document, and disseminate cybersecurity and privacy policies, procedures, processes, and guidance that must be developed, documented, disseminated, reviewed and update regularly. Remediation actions for violations of cybersecurity and privacy policies shall be defined and implemented.

(c) An organization-wide information security program plan that provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements must be developed and disseminated. This shall include the identification and assignment of roles and responsibilities and reflect the coordination among organizational entities responsible for information security.

(d) A comprehensive security governance structure that provides assurance that information security strategies are aligned with and support mission and business objectives must be implemented and consistent with applicable laws and regulations through adherence to policies and internal controls.

(e) Senior Agency Official for Privacy (SAOP) with the authority, mission, accountability, and resources to coordinate, develop, and implement applicable privacy requirements and manage privacy risks in accordance with VA's privacy program.

(f) Establish a principal governing body for its information security programs via a charter signed by the CIO. The principal governing body governs the management processes for information security and validates the effectiveness of those programs with a goal of continuously improving VA's security posture. This governing body serves as the VA Risk Executive Function.

(g) The Information Security Knowledge Service will be established as the approved source for VA cybersecurity and privacy policies, procedures, processes, and guidance. The Information Security Knowledge Service supports RMF practitioners by providing the approved access to VA security control baselines, security control descriptions, security control overlays, implementation guidance, and assessment procedures.

(h) Cybersecurity and privacy policies and capabilities must align with, and be mutually supportive of personnel, physical, and industrial information as well as operations security policies and capabilities.

(4) Risk Assessment

(a) An understanding of the cybersecurity and privacy risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals must be demonstrated.

(b) Risk assessments must be performed in accordance with NIST SP 800-30, NIST SP 800-53 and as described in the VA Information Security Knowledge Service. The risk factors described in NIST SP 800-30 and NIST SP 800-53 will be used across VA Administrations and Staff Offices to ensure ease of sharing risk information.

(c) Controls must be tailored and recommended by the risk assessments to accommodate resource constraints and the availability of detailed risk factor information (e.g. threat data). However, any tailoring must be clearly explained in risk assessment reports to ensure that Authorizing Officials (AO) understand to what degree they can rely on the results of the risk assessments.

(d) Systems, including those that operate in cloud environments, and applications must be monitored for new threats and scan the environment on an established schedule with agency-established criteria for performing special scans based on new threats.

(e) Contact groups and associations shall be selected and established within the security and privacy communities to share current security and privacy related information, including threats, vulnerabilities, and incidents; maintain currency with recommended security and privacy practices, techniques, and technologies; and facilitate ongoing security and privacy education and training for organizational personnel.

(f) Cybersecurity and privacy risks must be managed consistently across VA in a way that reflects organizational risk tolerance. Cybersecurity and privacy risk must be considered along with other organizational risks to ensure mission and business success.

(g) Plans of Action and Milestones (POA&Ms) process must be implemented to ensure that the security and privacy programs and associated organizational systems are developed and maintained. The POA&Ms document the remedial information security and privacy actions to adequately manage risk and implement remediation actions.

(h) VA will respond to findings from security and privacy assessments, monitoring, and audits in a POA&M. VA will manage the risk through strengthening existing controls or implementing new controls, accepting the risk with appropriate justification or rationale, sharing or transferring the risk, or rejecting the risk. If the risk response is to mitigate the risk and the mitigation cannot be completed immediately, a POA&M entry will be generated.

(i) All interconnections of VA IT must be managed to minimize shared risk by ensuring that the security posture of one system is not undermined by vulnerabilities of interconnected systems.

(5) Risk Management

(a) Priorities, constraints, risk tolerances, and assumptions must be established and used to support operational risk decisions.

(b) A multi-tiered cybersecurity and privacy risk management process described in NIST SP 800-39 and CNSS Policy (CNSSP No. 22) must be implemented to protect U.S. interests, VA operational capabilities, VA individuals, organizations, and assets.

(c) A comprehensive risk management strategy that defines how VA will manage security, privacy, and supply chain risk, including the determination of risk tolerance and the development and execution of organization-wide investment strategies for information resources and information security shall be published.

(d) VA will manage risk by identifying assumptions and constraints affecting risk assessments, risk response, and risk monitoring; the organizational risk tolerance; and priorities and trade-offs considered by the organization for managing risk.

(e) Information protection requirements will be satisfied by the selection and implementation of appropriate security and privacy controls in NIST SP 800-53, following the baselines defined in CNSSI No. 1253. Controls are implemented by common control providers, information system owners (ISOs), or program managers, and decisions are granted by AOs based on risk to the Department. Detailed guidance on system categorization and security control selection is provided in VA Handbook 6500 and on the Information Security Knowledge Service.

(f) Information systems will be designated as national security systems (NSS) or non-NSS systems according to criteria published on the Information Security Knowledge Service. NSS systems will require additional security measures. VA will incorporate risk management tasks throughout the system development life cycle.

(g) The security and privacy state of VA Information Systems and the environments (e.g. cloud environments) in which those systems operate will be managed throughout the authorization process. The authorization process is integrated with continuous monitoring processes to facilitate ongoing understanding and acceptance of security and privacy risks.

(h) Risk management continues during operations and sustainment, which may include the application of new or revised security or privacy controls prior to the integration of new IT services or products into an existing operational system, to maintain the security of the operational system.

b. Protect Function. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity and privacy event by developing and implementing the appropriate safeguards to ensure delivery of critical IT services. Outcome categories within the Protect Function include: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Media Sanitization; Maintenance; and Protective Technology; and associated activities, as described below:

(1) Identity Management and Access Control

(a) Access to physical and logical assets and associated facilities to authorized users, processes, and devices, and manage the assets consistent with the assessed risk of unauthorized access.

(b) Only VA-approved identity credentials will be used to authenticate entities requesting access. This requirement extends to all mission partners using VA IT.

(c) Public Key Infrastructure (PKI) solution will be enabled and implemented on VA Information Systems in accordance with current Federal requirements.

(d) A list of individuals with authorized access to VA facilities will be developed, approved, and maintained; authorization credentials will be issued for facility access.

(e) Usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed and authorized on VA Information Systems must be documented prior to allowing such connections.

(f) System access authorizations must be defined to support separation of duties.

(g) The principle of least privilege will be employed, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational mission and business functions.

(h) System components performing different missions or business functions will be isolated or segregated when necessary to limit unauthorized information flows among components and provide the opportunity to deploy greater levels of protection for selected system components.

(i) VA will proof identities and bind them to credentials and use this for assertion in interactions when appropriate, in accordance with current Federal requirements.

(2) Awareness and Training

(a) All authorized users of VA Information Systems will receive an initial Privacy and Information Security Awareness and Rules of Behavior orientation as a condition of access and, thereafter, participate annually in both VA and the Administration's enterprise cybersecurity and privacy awareness program.

(b) Cybersecurity and privacy awareness education and training shall be provided for organizational and non-organizational users to perform their information security-related duties and responsibilities and will be consistent with VA policies and procedures.

(c) A process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with VA Information Systems are developed, maintained, and executed in a timely manner must be implemented.

(d) Specialized training and awareness for privileged users, third-party stakeholders, and senior executives must be provided.

(e) Appropriate content for security and privacy training based on the assigned roles and responsibilities of individuals, specific VA security and privacy requirements, and the systems to which personnel have authorized access must be identified.

(3) Data Security

(a) Information, records, and data must be managed throughout the information life cycle consistent with VA's risk strategy to protect the confidentiality, integrity, and availability of information.

(b) Protect low, moderate and high impact CNSSI information at rest, in use and during transmission; this information shall be protected by encryption unless encrypting such information is technically infeasible or would demonstrably affect the ability of VA to carry out its missions, functions, or operations; and the risk of not encrypting is accepted by the AO and approved by the CIO, in consultation with the SAOP (as appropriate).

(c) A Data Governance Council (DGC) must be established and develop and implement guidelines supporting data modeling, quality, integrity, and de-identification needs of PII/PHI across the information life cycle.

(d) A Data Integrity Council shall be established to oversee organizational Computer Matching Agreements.

(e) VA IT that processes or stores PII or PHI, Payment Card Industry Data Security Standard (PCI-DSS) data, and VA Sensitive information will comply with appropriate VA policy.

(f) Cryptography required to protect VA information will be implemented in accordance with Federal Information Processing Standards (FIPS) 140-3.

(g) VA will protect against data breaches in accordance with NIST SP 800-37, NIST SP 800-39 and NIST SP 800-53.

(h) VA will employ integrity verification tools to detect unauthorized changes to selected software, firmware, hardware, and information.

(i) VA will protect against covert exfiltration of information.

(4) Information Protection Processes and Procedures

(a) Security policies that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities will be used and maintained to manage protection of information systems and assets.

(b) All VA IT will comply with applicable Security Technical Implementation Guides (STIGs) and security configuration guides, with any exceptions documented and approved by ISO and authorized by the responsible AO.

(c) Automation shall be used whenever possible in support of cybersecurity and privacy objectives, including, but not limited to, secure configuration management, continuous monitoring, active cyber defense, incident reporting, and situational awareness.

(d) Cybersecurity and privacy shall be fully integrated into system life cycles so that it will be a visible element of VA architectures, capability identification and development processes, integrated testing, IT portfolios, acquisition, operational readiness assessments, supply chain risk management, system security engineering (SSE), and operations and maintenance activities.

(e) Security and privacy control implementation, assessment, and sustainment shall be planned and budgeted throughout the system life cycle, including timely and effective configuration and vulnerability management.

(f) SSE principles and concepts will be used to design, develop, implement, modify, test, and evaluate information systems and system architectures as described in NIST SP 800-160.

(g) Proposed configuration-controlled changes to systems, must be reviewed, approved, or disapproved with explicit consideration for security impact analyses, and the decision must be documented.

(h) VA will conduct backups of user-level information and system-level information contained in VA Information Systems. System documentation will include security-related documentation.

(i) The confidentiality, integrity, and availability of backup information at storage locations must be protected in accordance with all VA policy.

(j) A physical security program must be established to protect VA IT from damage, loss, theft, or unauthorized physical access in accordance with VA policy.

(k) Policies and procedures must be updated to address system and organizational changes, or problems encountered during implementation, execution, or testing of the VA information security program.

(l) A threat awareness program will be implemented that includes a cross-organizational information sharing capability. Threat information sharing may be bilateral (e.g., government/commercial cooperatives) or multilateral (e.g., organizations taking part in threat-sharing consortia). Threat information may be highly sensitive, requiring special agreements and protection, or less sensitive and freely shared.

(m) Appropriate response and recovery plans must be developed, tested, implemented, managed and maintained. At a minimum, VA will manage, and test all plans on a yearly basis or when a significant change occurs, including incident response, business continuity, contingency, incident recovery, and disaster recovery plans.

(n) Cybersecurity and privacy workforce management policies and capabilities must be developed to support identification and qualifications for a professional cybersecurity and privacy workforce.

(o) System flaws will be identified, reported and corrected. Flaw remediation will be incorporated into VA's configuration management process.

(5) Media Sanitization

(a) Media sanitization on all electronic storage media must comply with NIST SP 800-88.

(b) A program must be maintained to sanitize and properly dispose of media containing VA sensitive information.

(c) Approved techniques or methods to retain VA information will be used consistent with VA retention guidelines and National Archives and Records Administration (NARA) approved records control schedules. This applies to originals as well as copies and archived records, including system logs that may contain PII/PHI PCI-DSS data and VA sensitive information.

(d) VA offices and facilities notified by the Office of General Counsel (OGC) that their IT equipment, electronic storage media, or information residing on either, is subject to retention for possible litigation purposes, must immediately cease the repair, reuse, disposal, destruction, or sanitization of the involved equipment, storage media, or data. These restrictions also apply to non-VA IT equipment (including research equipment and/or grant-owned equipment), electronic storage media, and VA information residing on either.

(e) Office of Information and Technology (OIT) staff will train Information System Security Officers (ISSOs) on VA data sanitization policies and procedures. They must also provide current copies of any VA policies and documents describing or depicting sanitization methods and procedures to appropriate staff members.

(f) Contracts involving media sanitization, electronic storage media, and IT equipment (e.g., sharing agreements and Memoranda of Understanding (MOU)), maintenance contracts, service contracts, and vendor repair agreements (including third party vendor repair and lease agreements) will comply with VA and Federal policy. These contracts must include the appropriate security language including HIPAA Security Rule requirements for ePHI concerning the protection of VA assets, including appropriate media sanitization for electronic storage media, IT systems and equipment.

(g) Users of non-VA leased or owned IT equipment including, but not limited to, personally-owned equipment (which requires an approved waiver from the VA AO), vendor-owned equipment, or research equipment obtained through a grant used to store, process, or access VA sensitive information are required to protect all VA sensitive information from subsequent disclosure to unauthorized persons during use and when the equipment is no longer used to access VA sensitive information.

(h) Returning leased equipment constitutes a risk. VA employees must sanitize VA sensitive information residing on leased equipment before releasing that equipment from direct VA control, or ensure the contract states the media will not be returned upon termination of the contract. Depending upon the contract, this may include VA licensed software installed on leased equipment. Copyright protected software must be removed from equipment prior to repair, disposal, or reuse unless it: (i) will be reused by an agency component included as a part of

the same group license under which the program was initially installed, or (ii) is required to ensure the repair was successful. If installing Commercial Off-the-Shelf (COTS) software, pre-approval is required by OIT and the Contracting Officer. If the COTS software requires a user license limited to that individual, the individual must remove that software from the machine before releasing the machine for another individual's use.

(i) When non-VA owned IT equipment is no longer used to access or store VA sensitive information, all equipment hard drives and internal memory is to be sanitized in accordance with VA policy. All other electronic storage media used to store, process, or access VA sensitive information must be sanitized in accordance with VA policy when the media are no longer used to access VA sensitive information being disposed of or removed from VA control.

(j) OIT and facility property managers are required to report usable excess IT equipment within VA and redistribute that equipment for use, if appropriate. If the excess IT equipment cannot be used within the agency, then donations of equipment to schools (grades K-12) are encouraged under the auspices of Executive Order 12999 (Computers for Learning Program), signed on April 16, 1996.

(k) OIT and facility property managers are encouraged to use VA's MOU established with UNICOR for processing scrap IT equipment and for the recycling of scrap electronic equipment in general. Electronic storage media/components will be removed prior to transfer to UNICOR and disposed of per NIST SP 800-88 for the purposes of media sanitization.

(6) Maintenance

(a) Maintenance and repairs of VA IT Information Systems and system components will be performed consistent with VA policies and procedures.

(b) Maintenance, repair, or replacements of system components will be scheduled, documented, managed and records reviewed in accordance with manufacturer or vendor specifications and/or organizational requirements. System maintenance also includes those components not directly associated with information processing and/or data or information retention, such as mobile devices, scanners, copiers, and printers.

(c) Maintenance activities will be approved and monitored whether performed on site or remotely and whether the system or system components are serviced on site or moved to another location, to ensure that VA sensitive information and PII is maintained under VA control.

(7) Protective Technology

(a) Technical security solutions will be managed to ensure the security and resilience of systems and assets are consistent with related policies, procedures, and agreements.

(b) System audit data will be collected and kept to support technical analysis relating to misuse, penetration, or other incidents involving IT under their purview, and provide this data to appropriate law enforcement or other investigating agencies as necessary.

(c) Technical and non-technical safeguards must be employed to limit the use of portable media, including digital (e.g., external or removable hard disk drives and flash drives) and non-digital media (e.g., paper and microfilm), and protect the portable media when not in use.

(d) Systems must be configured to provide only essential capabilities, and prohibit or restrict the use of selected functions, ports, protocols, and/or services.

(e) VA will monitor and control communications and networks at external boundaries and at key internal boundaries, and connect to external networks or systems only through managed interfaces.VA will pre-define functional states to achieve availability (e.g., under duress, under attack, during recovery, and normal operations) based on the criticality of the system to enable VA to complete its mission.

c. Detect Function. The Detect Function enables timely discovery of cybersecurity and privacy events by implementing the appropriate activities to identify the occurrence of a cybersecurity and privacy event. Outcome categories within the Detect Function include: Anomalies and Events; Security Continuous Monitoring; Detection Processes; and associated activities, as described below:

(1) Anomalies and Events

(a) Anomalous activities must be detected in a timely manner, in accordance with implementation guidance to determine the potential impact of the events on VA Information Systems and networks.

(b) Notify mission owners and network operators of the security posture of individual device or software objects to the aggregated systems of systems level.

(c) System security alerts, advisories, and directives from external organizations (e.g., US Computer Emergency Readiness Team (US-CERT)) must be received on an ongoing basis and generate internal security alerts, advisories, and directives as deemed necessary.

(d) Baseline configurations for systems and system components, including communications and connectivity-related aspects of systems will be established. Baseline configurations of systems reflect the current enterprise architecture and are required for all software approved for use at VA.

(e) Systems will be monitored to detect attacks, indicators of potential attacks, and unauthorized local, network, and remote connections.

(f) VA will track and document cybersecurity and privacy incidents in accordance with VA policy.

(g) Incident handling capability for security and privacy incidents will be implemented and will include preparation, detection and analysis, impact determination, containment, eradication, and recovery.

(h) The rigor, intensity, scope, and results of incident handling activities will ensure comparable and predictable results across the VA Administrations and Staff Offices.

(i) Incident information and individual incident responses will be aggregated to achieve an organization-wide perspective on incident awareness and response.

(j) The VA's incident response capability will issue an alert when system-generated indications of compromise or potential compromise occurs. Alerts may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers.

(2) Continuous Security Monitoring

(a) Information and assets will be monitored at discrete intervals to identify cybersecurity and privacy events and verify the effectiveness of protective measures.

(b) A security and privacy continuous monitoring strategy must be developed. VA will implement a security and privacy continuous monitoring program, in accordance with FISMA and for cloud systems Federal Risk and Authorization Management Program (FedRAMP), that assesses security and privacy controls and associated risks at a frequency sufficient to support risk management decisions. Having access to security- and privacy-related information on a continuing basis through reports and dashboards gives VA the capability to make more effective and timely risk management decisions, including ongoing authorization decisions.

(c) A continuous data monitoring capability will be established and maintained as specified in NIST SP 800-137 that provides cohesive collection, transmission, storage, aggregation, information sharing and presentation of data that conveys current operational status to affected VA stakeholders and VA's Federal and industry partners.

(d) Physical access to the facility where the system resides will be monitored to detect and respond to physical security incidents.

(e) Physical access authorizations will be enforced, and individual access authorizations verified before granting access to the facility to prevent unauthorized personnel from accessing VA facilities and systems.

(f) Personnel activity will be monitored to detect potential cybersecurity and privacy events.

(g) Insider threat controls will be implemented to detect and prevent malicious insider activity through the centralized integration and analysis of both technical and non-technical information to identify potential insider threat concerns in accordance with the VA Insider Threat Program.

(h) Malicious code protection mechanisms will be implemented at system entry and exit points to detect and eradicate malicious code, and automatically update malicious code protection mechanisms whenever new releases are available in accordance with guidance in the VA Information Security Knowledge Service.

(i) Acceptable and unacceptable mobile code and mobile code technologies must be defined. Usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies must be established. VA will also authorize, monitor, and control the use of mobile code within its systems.

(j) Providers of external system services will be required to comply with organizational security and privacy requirements. VA will monitor security and privacy control compliance by external service providers on an ongoing basis as is specified in VA Information Security Knowledge Service.

(k) Policy and procedures will be established to ensure that requirements for the protection of Controlled Unclassified Information (CUI) processed, stored, or transmitted on external systems are implemented in accordance with NIST SP 800-171.

(l) Through VA's Technical Reference Model (TRM), VA's Technical Reference Model, VA will continue to identify software programs authorized to execute on the system and employ an appropriate permission policy to maintain the capability for approved software.

(m) Network services that have not been authorized or approved must be detected.

(n) Automated mechanisms must be employed to detect the presence of unauthorized hardware, software, and firmware components within the system and take actions when unauthorized components are detected.

(o) VA will scan for vulnerabilities in the system and hosted applications as specified in the Information Security Knowledge Service, and when new vulnerabilities potentially affecting the system are identified and reported.

(3) Detection Processes

(a) Detection processes and procedures must be maintained and tested to ensure timely and adequate awareness of anomalous events.

(b) Personnel are required to report suspected security and privacy incidents to the organizational incident response capability.

(c) An incident response support resource, integral to the organizational incident response capability, which offers advice and assistance to users for the handling and reporting of security and privacy incidents must be provided.

(d) A process will be implemented to ensure that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems are developed, maintained, and continue to be executed in a timely manner.

d. Respond Function. The Respond Function supports the ability to contain the impact of a potential cybersecurity and privacy event and identifies the appropriate actions to take regarding the detected cybersecurity and privacy event. Outcome categories within the Respond Function include: Response Planning; Communications; Response and Recovery Analysis; Mitigation; Improvements; and associated activities, as described below:

(1) Response Planning

(a) An incident response plan will be developed and implemented that provides the organization with a roadmap for implementing its incident response capability. For incidents involving PII/PHI and PCI-DSS data, VA will include a process to determine whether notice to oversight organizations or affected individuals is appropriate and provide that notice accordingly.

(b) Response processes and procedures must be executed and maintained to ensure timely response to detected cybersecurity and privacy events.

(2) Communications

(a) VA response activities will be coordinated with internal and external stakeholders as appropriate, to include external support from law enforcement agencies.

(b) Responsibility for incident response in the Incident Response Plan will be explicitly designated.

(c) Personnel are required to report suspected security, privacy, and supply chain incidents.

(d) Internal stakeholders including, for example, mission/business owners, ISOs, AOs, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the Risk Executive Function, will coordinate to effectively handle incidents.

(e) Personnel on the alert notification list will be contacted when an alert or notification is issued. Personnel on the alert notification list can include, for

example, system administrators, mission or business owners, ISOs, ISSOs, or privacy officers.

(f) Incident information and individual incident responses must be correlated to achieve an organization-wide perspective on incident awareness and response.

(g) VA will coordinate with external organizations as defined in the Incident Response Plan to correlate and share incident information to achieve a cross-organizational perspective on incident awareness and more effective incident responses.

(3) Response and Recovery Analysis

(a) Analysis to ensure adequate response and support recovery activities must be conducted.

(b) Automated tools and mechanisms must be employed to support near real-time analysis of alerts and notifications generated by VA Information Systems.

(c) Incident response capability will be tested for the system to determine the incident response effectiveness and document the results.

(d) The impact of an incident on VA's mission and business practices must be determined.

(e) An integrated team of forensic and malicious code analysts, tool developers, and real-time operations personnel will be established to handle incidents and facilitate information sharing.

(f) VA will conduct forensic activities as defined in the VA Cybersecurity Incident Response Plan.

(g) Classes of incidents and the actions to take in response to those classes of incidents to ensure continuation of organizational mission and business functions.

(4) Mitigation

(a) Activities to prevent expansion of an event, mitigate its effects, and eradicate the incident must be performed.

(b) VA will mitigate risk of a security or privacy incident to VA by strengthening existing controls or implementing new controls, accepting the risk with appropriate justification or rationale, sharing or transferring the risk, or rejecting the risk.

(c) VA will accept the risk of newly identified security or privacy incidents. If the risk response is to mitigate the risk and the mitigation cannot be completed immediately, a POA&M will be generated in the authorization boundary where the risk is identified.

(d) Lessons learned from ongoing incident handling activities will be incorporated into incident response procedures, training, and testing; changes will be implemented accordingly.

(5) Improvements

(a) Organizational response activities will be improved by incorporating lessons learned from current and previous detection/response activities.

(b) Qualitative and quantitative data from incident response testing and actual events must be used to determine the effectiveness of incident response processes, continuously improve incident response processes incorporating advanced information security practices and provide incident response measures and metrics that are accurate, consistent, and in a reproducible format.

(c) The Incident Response Plan must be updated to address system and organizational changes, or problems encountered during plan implementation, execution, or testing, and communicate Incident Response Plan changes to incident response personnel and organizations.

e. Recover Function. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity and privacy event. Outcome Categories within the Recover Function include: Recovery Planning; Improvements; and Communications; and associated activities, as described below:

(1) Recovery Planning

(a) Necessary incident recovery plans will be defined and will be tested in accordance with Federal guidelines.

(b) Recovery processes and procedures will be executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity and privacy events in accordance with disaster recovery plans.

(c) Contingency plans will be developed using guidance found in NIST SP 800-34 that identifies essential mission and business functions and associated contingency requirements, and provides recovery objectives, restoration priorities, and metrics. The contingency plans also address maintaining essential mission and business functions despite a system disruption, compromise, or failure, and the eventual full system restoration without deterioration of the security and privacy controls originally planned and implemented.

(2) Improvements

(a) Recovery planning and processes will be improved by incorporating lessons learned into future activities.

(b) Contingency plans will be updated to address changes to the organization, system, or environment of operation, and problems encountered during

contingency plan implementation, execution, or testing, and communicate contingency plan changes to key contingency personnel and organizations.

(3) Communications

(a) Restoration activities will be coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacked systems, victims, other computer security incident response teams, and vendors.

(b) Communication with the public regarding cybersecurity and privacy incidents will be managed through the Office of Public and Intergovernmental Affairs (OPIA).

(c) VA reputation will be managed after an incident has been resolved through OPIA.

(d) VA will share information internally on recovery activities among organizational stakeholders, including, for example, executive and management teams, mission/business owners, ISOs, AOs, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the Risk Executive Function.

## 3. RESPONSIBILITIES.

a. **Secretary of Veterans Affairs.** The Secretary ensures agency compliance with requirements under 38 U.S.C. § 5723 and 44 U.S.C. § 3554.

b. **Inspector General of Veterans Affairs.** The Inspector General shall

(1) Carry out the responsibilities under 38 U.S.C. § 5723 and 44 U.S.C. § 3554.

(2) Ensure that organizations adhere to OMB, NIST and Federal regulations.

(3) Direct auditors, investigators, inspectors, and support personnel.

(4) Investigate, audit, inspect and evaluate all VA Information Systems.

c. **Assistant Secretary for Information and Technology, and Chief Information Officer (A/S OIT / CIO)** shall:

(1) Carry out the responsibilities under 38 U.S.C. § 5723 and 44 U.S.C. § 3554.

(2) Charter and co-chair the RMF TAG governing body.

(3) Monitor, evaluate, and provide advice to the Secretary of VA regarding all VA cybersecurity and privacy activities, and oversee implementation of this directive.

(4) Appoint a VA Chief Information Security Officer (CISO) in accordance with 44 U.S.C. § 3554.

(5) Direct and work with the OIT Deputy Chief Information Officer (DCIO) for Quality, Performance and Risk (QPR) to ensure that risk management strategies and policies are aligned with overarching VA cybersecurity and privacy strategy and VA business environments.

(6) Direct and work with the OIT DCIO for IT Resource Management (ITRM) to develop cybersecurity and privacy workforce management policies and capabilities to support identification and qualifications for a professional cybersecurity and privacy workforce.

(7) Direct and work with the Office of Human Resources & Administration Office of Operations, Security, and Preparedness (HR&A/OSP) to ensure that cybersecurity and privacy policies and capabilities are aligned with and mutually supportive of personnel, physical, industrial, information, and operations security policies and capabilities.

(8) Coordinate with the Office of Acquisition, Logistics, and Construction's (OALC) Executive Director to ensure that cybersecurity and privacy responsibilities are integrated into processes for VA acquisition programs, including research and development.

(9) Direct and coordinate with the Associate Deputy Assistant Secretary (ADAS) for IT Operations and Services (ITOPS) and ADAS for Enterprise Program Management Office (EPMO) to ensure that cybersecurity and privacy responsibilities are integrated into the operational testing and evaluation for VA programs.

(10) Co-chair the DGC that coordinates across VA, facilitates or oversees data quality and management activities, and develops and implements guidelines for data modeling, quality, integrity, designates authoritative data sources and appoints common information data stewards to monitor the linkages, de-identification, and access needs across the information life cycle.

(11) Direct, coordinate, and advocate resources for VA-wide cybersecurity and privacy solutions, including overseeing appropriations allocated to the VA cybersecurity and privacy program.

(12) Direct and coordinate with VA Administrations and Staff Offices to ensure that cybersecurity and privacy responsibilities are addressed for all VA IT.

(13) Integrate cybersecurity and privacy threat information sharing activities internal and external to VA to enhance VA cyber situational awareness.

(14) Develop policy for negotiating, performing, and concluding agreements with partners to engage in cooperative cybersecurity and privacy activities.

(15) Develop and implement policy regarding continuous monitoring of VA IT.

(16) Appoint in writing a trained and qualified AO for all VA IT systems operating within or on behalf of the CIO who is responsible for ensuring such systems are authorized in

accordance with this Directive. For VA Information Systems not under their purview (e.g., medical device systems), ensure that an AO is appointed by an equivalent departmental executive.

(17) Direct and coordinate with AO to ensure VA Information Systems within their purview are designated as NSS or non-NSS systems appropriately.

(18) Ensure all VA Information Systems are authorized to operate.

(19) Ensure an annual assessment of the VA cybersecurity and privacy program is conducted.

d. **Authorizing Official (AO)** shall:

(1) Make authorization decisions for VA Information Systems under their purview by formally assuming responsibility for operating VA Information Systems at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. In accordance with NIST SP 800-37, balancing security and privacy considerations with mission and business needs is paramount to achieving an acceptable risk-based authorization decision.

(2) Determine and designate VA Information Systems within their purview as NSS or non-NSS.

e. **Deputy Assistant Secretary (DAS) for Information Security.** Under the authority and direction of the VA CIO, the DAS for Information Security shall:

(1) Carry out the responsibilities under 38 U.S.C. § 5723 and 44 U.S.C. § 3554.

(2) Co-Chair the cybersecurity and privacy governing body.

(3) Develop a VA cybersecurity and privacy strategy that defines goals and objectives that, when implemented, guides and supports operational risk decisions.

(4) Develop and maintain cybersecurity and privacy policy in support of the cybersecurity and privacy program.

(5) Develop, implement, and manage cybersecurity and privacy for the VA enterprise network consistent with this directive and its supporting guidance.

(6) Develop or acquire solutions that support cybersecurity and privacy objectives for use throughout VA via the cybersecurity and privacy governing body process.

(7) Publish and maintain the VA Information Security Risk Management Strategy.

(8) Establish and maintain the VA Information Security Knowledge Service.

(9) Oversee and maintain the connection approval process in coordination with the Governance, Risk and Compliance tool committee and VA cybersecurity and privacy governing body, when appropriate.

(10) Facilitate information sharing efforts between VA and its Federal and industry partners in support of approved cybersecurity and privacy agreements.

(11) Ensure the continued development and maintenance of guidance and standard procedures to catalog, regulate, and control the use and management of Internet Protocols, data services, and associated ports on VA networks.

(12) Develop and establish a cybersecurity and privacy awareness program and role-based training for cybersecurity and privacy professionals.

(13) Support development of cybersecurity and privacy training and awareness products and a distributive training capability to support VA.

(14) Support training exercises, workforce development, network evaluation, and other efforts to build cybersecurity and privacy capacity.

(15) Coordinate with OSP to ensure cyber readiness inspection guidance and metrics provide a unity of effort among the security disciplines (i.e., personnel, physical, industrial, information, operations, and cybersecurity and privacy).

(16) Implement a process to ensure that POA&Ms and risks for the security and privacy programs and associated organizational systems are developed and maintained.

(17) Advise AOs, CIOs, ISSOs, and the Risk Executive Function on a range of security-related issues, including, for example, establishing information system boundaries and assessing the severity of weaknesses and deficiencies in the system, POA&Ms, risk mitigation approaches, security alerts, and potential adverse effects of identified vulnerabilities.

(18) Integrate policies established in this directive and its supporting guidance into acquisition policy, regulations, and guidance.

(19) Monitor and oversee all VA IT investments.

(20) Develop and implement a plan for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services.

f. **Chief Information Security Officer (CISO). On behalf of the VA CIO, the VA CISO** shall:

(1) Direct and coordinate the VA cybersecurity and privacy program and, as delegated, carry out the VA CIO's responsibilities pursuant to 44 U.S.C. § 3554 and 38 U.S.C. § 5723.

(2) Serve as the VA CIO's primary liaison to VA AOs, ISOs, and ISSOs.

(3) Ensure that VA IT is assigned to and governed by a VA cybersecurity and privacy program.

(4) Coordinate and liaise with NIST to ensure coordination and collaboration on NIST cybersecurity and privacy related issuances.

(5) Provide guidance and oversight in the development, submission, and execution of the VA cybersecurity and privacy program budget, and advocate for VA-wide cybersecurity and privacy solutions throughout the planning, programming, budget, and execution process.

(6) Develop guidance regarding how cybersecurity and privacy metrics are determined, established, defined, collected, and reported.

(7) Coordinate with DAS ITRM to integrate cybersecurity and privacy concepts into the VA acquisition process and address cybersecurity and privacy planning, implementation, and testing.

(8) Coordinate with DCIO QPR to ensure cybersecurity and privacy policies related to disclosure of sensitive information to international organizations is in accordance with VA policies and procedures.

(9) Develop VA-specific assignment values, implementation guidance, and validation procedures for security and privacy controls and publishes them in the Information Security Knowledge Service.

(10) Ensure VA IS contingency plans are developed and exercises are conducted to recover IS services following an emergency or IS disruption.

(11) Establish the RMF TAG established by this directive.

(12) Develop and provide policy for cybersecurity and privacy testing and evaluation during operational evaluations within VA, including describing the cybersecurity and privacy testing process clarified by updates in the ITOPS Memorandum.

(13) Conduct independent cybersecurity and privacy assessments during operational test and evaluation for systems and reports the findings.

(14) Review and approve, when appropriate, the cybersecurity and privacy operational test and evaluation documentation for all IT, IS, and special interest programs as required.

(15) Develop cybersecurity and privacy workforce management policies and capabilities.

(16) Provide enterprise security architecture and mechanisms to support business functions.

(17) Support the VA CIO by providing cybersecurity and privacy architecture and mechanisms to support business functions, including, but not limited to, cryptography, PKI, and SSE services.

(18) Provide cybersecurity and privacy support to VA in order to assess threats to, and vulnerabilities of, IT.

(19) Engage the cybersecurity and privacy industry and VA user community to foster development, evaluation, and deployment of cybersecurity and privacy solutions.

(20) Support the development of NIST publications and provide engineering support and other technical assistance for their implementation within VA.

(21) Provide SSE services, including describing information protection needs, properly selecting and implementing appropriate security and privacy controls, and assessing the effectiveness of system security.

(22) Develop SSE guidance at a design and architectural level and oversees continuing education requirements for all trained SSEs and cybersecurity and privacy architects throughout VA.

(23) Coordinate with information system owners, common control providers, and ISSOs on the allocation of security controls as system-specific, hybrid, or common controls.

(24) Advise AOs, CIOs, ISSOs, and the Risk Executive Function on a range of security-related issues, including, for example, establishing information system boundaries and assessing the severity of weaknesses and deficiencies in the system, POA&Ms, risk mitigation approaches, security alerts, and potential adverse effects of identified vulnerabilities.

(25) Provide a summary of security and privacy risk to the Authorizing Official.

g. **Deputy Assistant Secretary (DAS) for Development, Security and Operations (DevSecOps).** Under the authority and direction of the VA CIO, the DAS DevOps shall:

(1) Coordinate with the VA CIO to carry out the VA cybersecurity and privacy program responsibilities pursuant to 44 U.S.C. § 3554 and 38 U.S.C. § 5723.

(2) Ensure the Associate Deputy Assistant Secretary for EPMO and Associate Deputy Assistant Secretary for ITOPS carry out VA cybersecurity and privacy program responsibilities pursuant to 44 U.S.C. § 3554 and 38 U.S.C. § 5723.

h. **Associate Deputy Assistant Secretary (ADAS) for Enterprise Program Management Office (EPMO).** Under the authority and direction of the VA CIO, the ADAS EPMO shall:

(1) Exercise oversight responsibility for developmental test planning in support of interoperability, cybersecurity and privacy for programs acquiring VA IS.

(2) Establish procedures to ensure adequate development test and evaluation to support cybersecurity and privacy is planned, resourced, documented, and can be executed in a timely manner prior to approval of program documents.

(3) Ensure that IS requirements necessary to protect the organization's core mission and business processes are adequately addressed in all aspects of enterprise architecture, including reference models, segment and solution architectures, and the resulting information systems supporting those mission and business processes.

(4) Follow VA cybersecurity and privacy policies, procedures, processes, and guidance published on the Information Security Knowledge Service and validate that any EPMO-specific guidance is consistent with guidance on the Information Security Knowledge Service.

(5) Review and approve, when appropriate, all applications of cryptographic algorithms for the protection of sensitive information.

i. **Associate Deputy Assistant Secretary (ADAS) for IT Operations and Services (ITOPS).** Under the authority and direction of the VA CIO, the ADAS for ITOPS shall:

(1) Ensure that all VA IT under their purview complies with applicable security configuration guides, with any exceptions documented and approved by the responsible AO.

(2) Ensure identified critical system assets supporting essential mission and business functions are safeguarded and countermeasures can be employed.

(3) Ensure that cybersecurity and privacy requirements are addressed and visible in all capability portfolios, IT life cycle management processes, and investment programs incorporating IT.

(4) Plan, design, manage, and execute the development and implementation of PKI within VA, in coordination with OIS.

(5) Approve all applications of cryptographic algorithms for the protection of sensitive information.

(6) Conduct criticality analysis when an architecture or design is being developed to identify critical system components and functions.

(7) Ensure that cybersecurity and privacy requirements are addressed and visible in all capability portfolios, IT life cycle management processes, and investment programs incorporating IT.

j. **Cyber Security Operations Center (CSOC).** Under the direction of the DCIO OIS for Information Security, the VA CSOC shall:

(1) Coordinate the cybersecurity incident response when an event transitions to a cyber incident.

(2) Serve as the authoritative source for addressing and managing a cybersecurity breach or attack (also known as a cyber incident) to contain and limit the damage and reduce recovery time and cost.

(3) Issue an alert when system-generated indications of compromise or potential compromise occur.

(4) Contact personnel on the alert notification list when an alert or notification is issued.

(5) Implement a threat program that includes a cross-organization and cross-discipline incident handling team and information sharing capability.

(6) Conduct digital media analysis for forensic activities as defined in the VA Cybersecurity Incident Response Plan.

(7) Establish an integrated team of forensic and malicious code analysts, tool developers, and real-time operations personnel to handle incidents and facilitate information sharing.

(8) Identify classes of incidents and the actions to take in response to those classes of incidents to ensure continuation of organizational mission and business functions.

(9) Work with Department of Homeland Security (DHS) to periodically test VA's external and internal security posture.

(10) Share relevant, actionable, and valuable cyber threat intelligence with stakeholders.

(11) Provide enterprise-level vulnerability and compliance scanning.

(12) Detect cyber threat activity on VA network, Cyber Insider Threat, Forensics and malware analysis.

(13) Track and report critical findings, Federal mandates and security metrics.

(14) Report security incidents, including containment; eradication recommendations; lessons learned and after-actions to DHS and the Office of Inspector General.

k. **Deputy Chief Information Officer (DCIO) for Quality, Performance and Risk (QPR)** shall:

(1) Align cybersecurity and privacy strategies, policies, and capabilities with policies and capabilities relating to the disclosure of sensitive information.

(2) Negotiate, perform, and conclude agreements with stakeholders to engage in cooperative cybersecurity and privacy activities.

(3) Develop and maintain VA's Risk Management Strategy.

l. **Under Secretaries, Assistant Secretaries, and Other Key Officials** shall:

(1) Carry out their responsibilities under 38 U.S.C. § 5723 and 44 U.S.C. § 3554.

(2) Ensure that IT under their purview complies with this directive, including designation of AOs for systems under their purview.

(3) Direct and coordinate with AO to ensure VA Information Systems within their purview are designated as NSS or non-NSS systems appropriately.

(4) Ensure that cybersecurity and privacy requirements are addressed and visible in all capability portfolios, IT life cycle management processes, and investment programs incorporating IT.

(5) Ensure VA mission and business processes are defined with consideration for information security and privacy, the resulting risk, and determine information protection and PII/PHI processing needs arising from the defined mission and business processes.

(6) Participate in the cybersecurity and privacy governing body and ensure solutions that support the cybersecurity and privacy objectives are implemented.

(7) Ensure that contracts and other agreements include specific requirements to provide cybersecurity and privacy for VA information and the IT used to process that information in accordance with this directive.

(8) Ensure that all personnel with access to VA IT are appropriately cleared and qualified under the provisions of VA policy and that access to all VA IT processing specified types of information (e.g., PII and PHI) under their purview is authorized.

(9) Ensure that personnel occupying cybersecurity and privacy positions are assigned in writing, trained and qualified, assigned a position sensitivity designation, and meet the associated suitability and fitness requirements in accordance with VA policy.

(10) Use VA cybersecurity and privacy training in addition to awareness products, and ensure all staff take security awareness training annually, at a minimum, to meet the baseline user awareness training required in VA cybersecurity and privacy policy.

(11) Ensure that cybersecurity and privacy solutions do not unnecessarily restrict the use of assistive technology by individuals with disabilities, or access to/use of information and data by individuals with disabilities, in accordance with 29 U.S.C §§ 791, 794, and 794d.

(12) Be responsible and accountable for the implementation of VA security requirements in accordance with this directive and supplemental VA guidance.

(13) Ensure that personnel are considered for administrative or judicial sanctions if they knowingly, willfully, or negligently compromise, damage, or place at risk VA information.

(14) Implement cybersecurity and privacy capabilities responsive to VA requirements.

(15) Ensure that maintenance and disposal of information on VA IT complies with the provisions of VA policies and procedures.

m. **Principal Deputy Assistant Secretary for Operations, Security, and Preparedness (OSP)** shall:

(1) Coordinate with the VA CIO on development and implementation of cybersecurity and privacy policy, guidance, procedures, and controls related to operations, security, and preparedness.

(2) Implement an insider threat program that includes a cross-discipline insider threat incident handling team.

(3) Establish a physical security policy to protect VA IT from damage, loss, theft, or unauthorized physical access.

(4) Coordinate with OIS to ensure cyber readiness inspection guidance and metrics provide a unity of effort among the security disciplines (i.e., personnel, physical, industrial, information, operations, and cybersecurity).

n. **Assistant Secretary for Enterprise Integration (OEI)** shall:

(1) Establish and co-chair a DGC that coordinates across VA, facilitates or oversees data quality and management activities, and develops and implements guidelines for data modeling, quality, integrity, designates authoritative data sources and appoints common information data stewards to monitor the linkages, de-identification, and access needs across the information life cycle.

(2) Oversee and manage all data sharing agreements internal and external to VA.

(3) Coordinate with OIT to ensure that the enterprise level cybersecurity and privacy risks are appropriately represented in the VA Enterprise Risk Management (ERM) Risk Profile and/or Risk Register as required by OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control.

o. **Senior Agency Official for Privacy (SAOP)** shall:

(1) Ensure that all VA regulations and policies consider and address privacy implications.

(2) Oversee, coordinate, and facilitate the VA's privacy compliance efforts.

(3) Manage VA privacy risks associated with any VA activity that involves the creation, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII/PHI by programs and information systems.

(4) Review privacy risks beginning at the earliest planning and development stages and continues throughout the life cycle of programs and information systems.

(5) Review and approve as appropriate: (i) the categorization of information systems that handle PII, (ii) privacy plans for agency information systems prior to authorization, reauthorization, or ongoing authorization, and (iii) authorization

packages for information systems that handle PII; prior to AOs making risk determinations and acceptance decisions.

(6) Ensure that appropriate notice of privacy rights and monitoring policies are provided to all individuals accessing VA Administration and Staff Office-owned or controlled VA Information Systems.

(7) Establish a Data Integrity Board to oversee organizational Computer Matching Agreements.

(8) Ensure that a mechanism is in place to assess the quality and thoroughness of each PIA.

p. **Information System Owners (ISOs) and/or Technical Data Stewards** shall:

(1) Carry out their responsibilities under 38 U.S.C. § 5723.

(2) Plan and budget for security and privacy control implementation, assessment, and sustainment throughout the system life cycle, including timely and effective configuration and vulnerability management.

(3) Ensure that SSEs are consulted in the design, development, implementation, modification, test, and evaluation of the system architecture in compliance with the cybersecurity and privacy component of the VA Enterprise Architecture and to make maximum use of enterprise cybersecurity and privacy.

(4) Coordinate with VA Administrations and Staff Offices as well as VA procurement practices and policies prior to the acquisition of IT or the integration of IT into information systems when required.

(5) Ensure systems are identified, designated as such, and centrally registered in the VASI.

(6) Ensure that users are compliant with VA policies and procedures governing the generation, collection, processing, dissemination, and disposal of specified information.

(7) Comply with the rules for appropriate use and protection of information that is shared, processed, stored or transmitted within VA.

q. **Information System Security Officers (ISSOs)** shall:

(1) Ensure that all VA Information Systems are compliant with the cybersecurity and privacy policies and procedures and provide guidance to the ISO.

(2) Ensure that all users have completed the VA Privacy and Information Security Awareness and Rules of Behavior training before access is granted for VA Information Systems under their purview.

(3) Verify that all VA IS security documentation is current and accessible to properly authorized individuals.

(4) Verify that authorized users and support personnel receive appropriate cybersecurity and privacy training.

(5) Be the points of contact for the Media Sanitization program and audit all phases of the program for each Administration and Staff Office.

r. **Privileged Users.** Privileged Users (e.g., System Administrators) shall:

(1) Utilize Privileged Users permissions only when needed to perform a required task.

(2) Ensure that assigned IT systems are configured and operated in accordance with VA cybersecurity and privacy policies and procedures.

(3) Notify the responsible ISSO of any changes that might affect security posture.

(4) Comply with the responsibilities of Privileged Authorized Users.

s. **Authorized Users.** Authorized Users (e.g., general users) shall:

(1) Carry out their responsibilities under 38 U.S.C. § 5723.

(2) Comply with all Department IS program policies, procedures, and practices.

(3) Complete the annual Security Awareness training and sign the VA Rules of Behavior.

## 4. REFERENCES.

a. **Statutes and Regulations**

(1) 38 U.S.C. § 5723, *Responsibilities*.

(2) 40 U.S.C. § 11313, *Performance and results-based management*.

(3) *Health Insurance Portability and Accountability Act (HIPAA), Pub. L. 104-191, 110 Stat. 1936 (1996)*.

(4) 42 U.S.C. § 17901-17903, *Health Information Technology for Economic and Clinical Health Act (HITECH)*.

(5) 44 U.S.C. § 3551 – 3558, *Federal Information Security Modernization Act (FISMA)*.

(6) 44 U.S.C. § 3554, *Federal Agency Responsibilities*.

(7) Exec. Order No. 13800, 82 FR 22391, *Strengthening the Cybersecurity of Federal networks and Critical Infrastructure,* May 11, 2017.

b. **Federal Information Processing Standards (FIPS) Publications**

(1) FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*.

(2) FIPS 140-3, *Security Requirements for Cryptographic Modules*.

(3) FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*.

c. **National Institute of Standards and Technology (NIST)**

(1) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Guide for Conducting Risk Assessments*.

(2) NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*.

(3) NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*.

(4) NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*.

(5) NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*.

(6) NIST SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*.

(7) NIST SP 800-59, *Guideline for Identifying an information System as a National Security System*.

(8) NIST SP 800-63-3, *Digital Identity Guidelines*.

(9) NIST SP 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*.

(10) NIST SP 800-88, *Guidelines for Media Sanitization*.

(11) NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*.

(12) NIST SP 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*.

(13) NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*.

(14) NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, v1.1, April 16, 2018.

d. **Committee on National Security System Instructions (CNSSI and Policies)**

(1) Committee on National Security System Instruction 1253, *Security Categorization and Control Selection for national Security Systems.*

(2) Committee on National Security System Instruction 4009, *Committee on National Security Systems (CNSS) Glossary*.

(3) Committee on National Security System Policy 22, *Cybersecurity Risk Management Policy*.

e. **Office of Management and Budget (OMB) Publications**

(1) OMB Circular A-19, *Legislative Coordination and Clearance*, September 20, 1979.

(2) OMB Circular A-130, *Managing Information as a Strategic Resource,* July 28, 2016.

(3) OMB M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government,* October 30, 2015.

(4) OMB M-16-24, *Role and Designation of Senior Agency Officials for Privacy*, September 15, 2016.

f. **VA Policy**

(1) VA Directive 6518, Enterprise Information Management (EIM), February 20, 2015.

(2) Data Governance Council Charter, May 19, 2017.

(3) Internet X. 509 Public Key Infrastructure (PKI) Certificate Management Protocols Standard, March 1999.

(4) VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, October 26, 2015.

(5) VA Directive 6513, Secure External Connections, October 12, 2017.

(6) VHA Directive 6300, Records Management, October 22, 2018.

(7) VA Directive 6502, VA Enterprise Privacy Program, May 5. 2008.

(8) VA Directive 0327, Insider Threat Policy, February 05, 2015.

(9) VA Handbook 0327, Insider Threat Program, April 10, 2017.

(10) VA Information Security Knowledge Service, VA Information Security Knowledge Service.

(11) VA Technical Reference Model (TRM), VA's Technical Reference Model.

**5. DEFINITIONS.** Unless otherwise noted, these terms and their definitions are for the purposes of this directive.

a. **Application:** A software program hosted by an information system. SOURCE: NIST SP 800-37

b. **Authoritative Source:** An entity that has access to, or verified copies of, accurate information from an issuing source such that a Cloud Service Provider can confirm the validity of the identity evidence supplied by an applicant during identity proofing. An issuing source may also be an authoritative source. Often, authoritative sources are determined by a policy decision of the agency or Cloud Service Provider before they can be used in the identity proofing validation phase. SOURCE: NIST SP 800-63-3

c. **Authorized User:** Individual, or (system) process acting on behalf of an individual, authorized to access an information system. SOURCE: NIST SP 800-53

d. **Availability:** Ensuring timely and reliable access to and use of information. SOURCE: NIST SP 800-53

e. **Business Owner:** See Mission Owner.

f. **Chief Information Security Officer (CISO):** Official responsible for carrying out the CIO's responsibilities under the Federal Information Security Modernization Act (FISMA) and serving as the CIO's primary liaison to the agency's AOs, information system owners, and ISSOs. SOURCE: NIST SP 800-53

g. **Computer Matching Agreements:** An agreement entered into by an organization in connection with a computer matching program to which the organization is a party, as required by the Computer Matching and Privacy Protection Act of 1988. With certain exceptions, a computer matching program is any computerized comparison of two or more automated federal systems of records or a system of records with nonfederal records for the purpose of establishing or verifying the eligibility of, or continuing compliance with, statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to cash or in-kind assistance or payments under federal benefit programs or computerized comparisons of two or more automated federal personnel or payroll systems of records or a system of federal personnel or payroll records with non-federal records.. SOURCE: NIST SP 800-53

h. **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. SOURCE: NIST SP 800-53

i. **Continuous monitoring:** Maintaining ongoing awareness to support organizational risk decisions. SOURCE: NIST SP 800-137

j. **Controlled Unclassified Information (CUI):** Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or disseminating controls. Excludes information that is required to be marked classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended. SOURCE: 32 C.F.R. Part 2002 and NIST SP 800-171

k. **Cybersecurity:** Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. SOURCE: NIST SP 800-53 and OMB Circular A-130

l. **Data Governance Council (DGC):** The VA Data Governance Council (DGC) implements the requirements of VA Directive 6518, Enterprise Information Management (EIM) for the management of VA common data and provides a forum to share and integrate data management best practices across common and Administration and Staff Office shared and organizational specific data domains. SOURCE: Data Governance Council signed by VA Chief of Staff (COS) on May 19, 2017

m. **Information Flow Control:** Procedure to ensure that information transfers within an information system are not made in violation of the security policy. SOURCE: CNSSI 4009-2015

n. **Information System Life Cycle:** The stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage and disposition. SOURCE: OMB Circular A-130

o. **Information Resource:** Information and related resources, such as personnel, equipment, funds, and information technology. SOURCE: NIST SP 800-53

p. **Information Security Knowledge Service:** The VA's knowledge portal for providing cybersecurity and privacy policies, procedures, and guidance.

q. **Information Stewards:** An agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. SOURCE: CNSSI 4009

r. **Information System Security Officer (ISSO):** Individual assigned responsibility by the senior agency ISSO/CISO, AO, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program. SOURCE: NIST SP 800-53A

s. **Information System (IS):** A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. SOURCE: NIST SP 800-53

t. **Information System Owner:** Person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system. SOURCE: CNSSI 4009-2015

u. **Information Technology (IT):** Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term IT includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. SOURCE: NIST SP 800-53

v. **Information Technology (IT) Service:** A capability provided to one or more VA entities by an internal or external provider based on the use of IT and supporting a VA mission or business process. An IT Service consists of a combination of people, processes, and technology.

w. **Insider Threat:** An entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service. SOURCE: CNSSI 4009

x. **Integrity:** Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. SOURCE: NIST SP 800-53

y. **Mission Owner:** The mission owner, also referred to as business owner, is the senior official or executive within an organization with specific mission or line of business responsibilities and that has a security or privacy interest in the organizational systems supporting those missions or lines of business. SOURCE: NIST SP 800-37

z. **Mission Partners:** Those with whom VA cooperates to achieve goals, such as other departments and agencies of the U.S. Government, state and local governments, non-governmental organizations, and the private sector.

aa. **Mobile Code:** Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. SOURCE: NIST SP 800-53

bb. **National Security System:** Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency – (i) the function, operations, or use of which (I) involves intelligence activities; (II) involves cryptologic activities related to national security; (III) involves command and control of military forces; (IV) involves equipment that is an integral part of a weapon or weapons systems; or (V) is critical to the direct fulfilment of a military or intelligence missions or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order an Act of Congress to be kept classified in the interest of national defense or foreign policy. Subparagraph (i) (V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). SOURCE: 44 U.S.C. SEC 3542 (b) (2).

cc. **Network:** Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. SOURCE: NIST SP 800-53

dd. **Operational Resilience:** The ability to quickly adapt and recover from any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning. SOURCE: NIST SP 800-34

ee. **Overlay:** A specification of security controls, control enhancements, supplemental guidance, and other supporting information developed for specific types of information or communities of interest, employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems. SOURCE: CNSSI 4009 and OMB A-130

ff. **Payment Card Industry Data Security Standard (PCI DSS):** PCI-DSS is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

gg. **Personally, Identifiable Information (PII):** Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Examples of PII elements include but are not limited to name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

hh. **Privacy Controls:** Technical and non-technical controls which support a variety of specialty applications, including the Risk Management Framework and Cybersecurity Framework, to protect organizations, systems, and individuals. SOURCE: NIST SP 800-53

ii. **Privileged User:** A user that is authorized (and, therefore, trusted) to perform security – relevant functions that ordinary users are not authorized to perform. SOURCE: NIST SP 800-53

jj. **Program Manager:** Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. SOURCE: NIST SP 800-53

kk. **Protected Health Information (PHI):** Protected Health Information, is considered a subcategory of PII. This term applies only to individually identifiable health information that is under the control of VHA, as VA's only Covered Entity under HIPAA. PHI is health (including demographic) data that is transmitted by, or maintained in, electronic or any other form or medium. PHI excludes employment records held by an employer in its role as employer, records of a person deceased for more than 50 years, and some education records. It includes genetic information.

ll. **Public Key Enabling:** The incorporation of the use of certificates for security services such as authentication, confidentiality, data integrity, and non-repudiation. SOURCE: CNSSI 4009

mm. **Risk Executive Function**: An individual or group within an organization that helps to ensure that: (i) security risk-related considerations for individual information systems, to include the authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its mission and business functions, and (ii) managing risk from individual information systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success. SOURCE: NIST SP 800-37

nn. **Security Controls**: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. SOURCE: NIST SP 800-53

oo. **Security Posture:** The security status of an enterprise's networks, information, and systems based on information assurance resources (e.g., people, hardware, software, and policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes. SOURCE: CNSSI 4009

pp. **Senior Agency Official for Privacy (SAOP):** The VA SAOP must be a senior official at the Deputy Assistant Secretary (DAS) or equivalent level with the necessary skills, knowledge, and expertise to lead and direct the VA's privacy program.

qq. **Supply Chain Risk:** The risk that an adversary may sabotage, maliciously introduce unwanted functions, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of an item of supply or a system to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of a system. SOURCE: CNSSI 4009

rr. **System Development Life Cycle:** The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation. SOURCE: NIST SP 800-34

ss. **VA-controlled:** Used only for VA purposes, dedicated to VA processing, and effectively under VA configuration control.

tt. **VA Sensitive Information:** Any information that has not been cleared for public release and has been collected, developed, received, transmitted, used, or stored by VA, or by a non-VA entity in support of an official VA activity. VA Sensitive Information may be a type of Controlled Unclassified Information (CUI), and if so, must follow the VA's CUI guidance.

uu. **VA IS:** VA-owned IS and VA-controlled IS. A type of VA IT.

vv. **VA IT:** VA-owned IT and VA-controlled IT.