**DEPARTMENT OF VETERANS AFFAIRS**
**Washington, DC 20420**

**VA DIRECTIVE 6500**
**Transmittal Sheet**
**January 23, 2019**

# VA CYBERSECURITY PROGRAM

1. **REASON FOR ISSUE:** Reissues VA Directive 6500 pursuant to the authority to maintain a VA cybersecurity program to protect and defend VA information and information technology (IT) that is consistent with VA's information 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.

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

   a. Establishes the governance structure as the Risk Executive Function;

   b. Establishes the Risk Management Framework (RMF) Technical Advisory Group (TAG), which serves as the governing body for security control management and implementation;

   c. Establishes the Information Security Knowledge Service (KS) to provide cybersecurity policies, procedures, and guidance; and

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

3. **RESPONSIBLE OFFICE:** Office of the Assistant Secretary for Information and Technology (005) and Office of Information Security (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 September 20, 2012 and VA Handbook 6500.1, Electronic Media Sanitization**,** dated November 3, 2008.

**CERTIFIED BY:**

/s/
Melissa S. Glynn, Ph.D.
Assistant Secretary for
Enterprise Integration

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

/s/
James R. Gfrerer
Assistant Secretary for Information and Technology and
Chief Information Officer

**DISTRIBUTION**: Electronic Only

This page is intentionally blank.

VA CYBERSECURITY PROGRAM

## 1. PURPOSE.

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

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

b. Establishes a governance structure as the security Risk Executive Function;

c. Establishes the Information Security Program Risk Management Framework (RMF) Technical Advisory Group (TAG) to strengthen VA's ability to rapidly deploy secure systems;

d. Establishes the Information Security Knowledge Service (KS) to provide cybersecurity policies, procedures, and guidance; and

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

## 2. POLICY.

**VA Cybersecurity Program.** VA will use this directive as well as the RMF as defined in NIST Special Publication (SP) 800-37, and as implemented by VA Handbook 6500 and the security control baselines in NIST SP 800-53. This information will be located on the VA KS.

The five core cybersecurity functions that define the VA cybersecurity 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 the 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 risk to systems, assets, data, and capabilities, and identify any gaps in VA's cybersecurity practices. Outcome categories within the Identify Function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy; and associated activities, as described below:

(1) Asset Management

(a) VA will identify and manage all assets (e.g., data, personnel, devices, systems, and facilities) consistent with their relative importance to VA business objectives and risk strategy.

(b) All VA ISs will be registered in the VA Systems Inventory (VASI) in accordance with VA policy and will be registered as part of a security accreditation in VA's Governance, Risk and Compliance tool committee.

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

(d) VA will develop information flow control policies and enforce approved authorizations for controlling the flow of information within the system and between interconnected systems.

(e) VA will assign an appropriate level of confidentiality, integrity, and availability to all VA information in electronic format that reflects the importance of both information sharing and protection.

(2) Business Environment

(a) VA will use its understanding of its three major business environments (health, benefits, and memorial affairs) and support functions to inform cybersecurity roles and responsibilities, and make informed risk management decisions.

(b) VA will define its mission and business processes with consideration for information security and privacy and the resulting risk, and determine information protection, Personally Identifiable Information (PII), and Protected Health Information (PHI) processing needs arising from the defined mission and business processes.

(c) VA will develop and implement a plan for managing financial and supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services.

(d) VA will develop, document, and regularly update VA's critical infrastructure and key resources protection plan, and address information security and privacy issues in the plan.

(e) VA will identify critical system assets supporting essential mission and business functions so additional safeguards and countermeasures can be employed as needed. The identification of critical information assets also facilitates the prioritization of organizational resources.

(f) VA will perform a criticality analysis when an architecture or design is being 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 will be 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.

(h) VA will implement cybersecurity solutions consistent with enterprise architecture principles and guidelines within the VA Architecture Framework and VA cybersecurity architectures developed or approved by the VA Chief Information Officer (CIO).

(i) VA will implement operational resilience 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) VA will define resiliency requirements to support the delivery of critical services during all operating states (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.

(3) Governance

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

(b) VA will develop, document, and disseminate cybersecurity policies, procedures, processes, and guidance, and review and update them regularly. VA will define and implement remediation actions for violations of cybersecurity policies.

(c) VA will develop and disseminate 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, the identification and assignment of roles and responsibilities, and reflecting the coordination among organizational entities responsible for information security.

(d) VA will implement a comprehensive security governance structure that provides assurance that information security strategies are aligned with and support mission and business objectives, and are consistent with applicable laws and regulations through adherence to policies and internal controls.

(e) VA will appoint a 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 through an organization-wide privacy program.

(f) VA will 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 as described in NIST SP 800-37 and NIST SP 800-39.

(g) VA will establish the RMF TAG to support the VA Chief Information Security Officer (CISO). The RMF TAG serves as the governing body for security control management and implementation.

(h) VA will establish the Information Security KS as the authoritative source for VA cybersecurity policies, procedures, processes, and guidance. The KS supports RMF practitioners by providing access to VA security control baselines, security control descriptions, security control overlays, implementation guidance, and assessment procedures.

(i) VA will align cybersecurity policies and capabilities with, and be mutually supportive of, personnel, physical, and industrial information and operations security policies and capabilities.

(4) Risk Assessment

(a) VA will demonstrate understanding of the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

(b) VA will perform risk assessments in accordance with NIST SP 800-30 and as described in the VA KS. The risk factors described in NIST SP 800-30 will be used across VA Administrations and Staff Offices to ensure ease of sharing risk information.

(c) VA will tailor the rigor of 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) VA will monitor systems and hosted applications for new threats and scan the environment on an established schedule with agency-established criteria for performing special scans based on new threats.

(e) VA will establish and institutionalize contact with selected groups and associations 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) VA will manage cybersecurity risks consistently across VA in a way that reflects organizational risk tolerance and is considered along with other organizational risks to ensure mission and business success.

(g) VA will implement a process to ensure that Plans of Action and Milestones (POAMs) for the security and privacy programs and associated organizational systems are developed and maintained. The POAMs document the remedial information security and privacy actions to adequately respond to risk.

(h) VA will respond to findings from security and privacy assessments, monitoring, and audits by managing 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 POAM entry will be generated.

(i) VA will manage all interconnections of VA IT 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) VA will establish priorities, constraints, risk tolerances, and assumptions, and use them to support operational risk decisions.

(b) VA will implement a multi-tiered cybersecurity risk management process to protect U.S. interests, VA operational capabilities, and VA individuals, organizations, and assets as described in NIST SP 800-39.

(c) VA will publish 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.

(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) VA will satisfy information protection requirements by the selection and implementation of appropriate security and privacy controls in NIST SP 800-53. Controls are implemented by common control providers, system owners (SOs), or program managers, and risk-based authorization decisions are granted by AOs. Detailed guidance on system categorization and security control selection is provided in VA Handbook 6500.

(f) VA will begin risk management tasks early in the system development life cycle.

(g) VA will manage the security and privacy state of VA systems and the environments in which those systems operate 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) VA continues risk management 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 event by developing and implementing the appropriate safeguards to ensure delivery of critical IT services. Outcome categories within the Protect Function include: Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology; and associated activities, as described below:

(1) Identity Management and Access Control

(a) VA will limit 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) VA IT will use only VA-approved identity credentials to authenticate entities requesting access. This requirement extends to all mission partners using VA IT.

(c) VA will public key-enable VA ISs and implement a VA-wide Public Key Infrastructure (PKI) solution that will be managed by the VA PKI Program Management Office.

(d) VA will develop, approve, and maintain a list of individuals with authorized access to VA facilities and issue authorization credentials for facility access.

(e) VA will document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed, and authorize remote access to VA systems prior to allowing such connections.

(f) VA will define system access authorizations to support separation of duties.

(g) VA will employ the principle of least privilege, 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) VA will isolate or segregate system components performing different missions or business functions 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 will use this for assertion in interactions when appropriate.

(2) Awareness and Training

(a) All authorized users of VA IS will receive an initial cybersecurity awareness orientation as a condition of access and, thereafter, participate annually in both VA and the Administration's enterprise cybersecurity awareness program.

(b) VA will provide VA personnel and partners with cybersecurity awareness education and training to perform their information security-related duties and responsibilities consistent with VA policies, procedures, and agreements.

(c) VA will implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with VA systems are developed, maintained, and executed in a timely manner.

(d) VA will provide specialized training and awareness for privileged users, third-party stakeholders, and senior executives.

(e) VA will identify 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.

(3) Data Security

(a) VA will manage information, records, and data throughout the information life cycle consistent with VA's risk strategy to protect the confidentiality, integrity, and availability of information. Federal Register Volume 67, Number 36 (Friday, February 22, 2002)]

(b) VA will protect moderate and high impact information at rest and during transmission 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) VA will establish a Data Management Board and develop and implement guidelines supporting data modeling, quality, integrity, and de-identification needs of PII/PHI across the information life cycle.

(d) VA will establish a Data Integrity Board to oversee organizational Computer Matching Agreements.

(e) VA IT that processes or stores PII or PHI will comply with appropriate VA policy.

(f) Cryptography required to protect VA information will be implemented in accordance with Federal Information Processing Standards (FIPS) 140-2.

(g) VA will protect against data breaches.

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

(4) Information Protection Processes and Procedures

(a) VA will use and maintain security policies that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities to manage protection of information systems and assets.

(b) All VA IT will comply with applicable security configuration guides, with any exceptions documented and approved by the responsible AO.

(c) VA will use automation whenever possible in support of cybersecurity objectives, including, but not limited to, secure configuration management, continuous monitoring, active cyber defense, incident reporting, and situational awareness.

(d) VA will fully integrate cybersecurity 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) VA will 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.

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

(g) VA will review proposed configuration-controlled changes to systems, approve or disapprove such changes with explicit consideration for security impact analyses, and document the decision.

(h) VA will conduct backups of user-level information and system-level information contained in VA systems, and conduct backups of system documentation including security-related documentation.

(i) VA will protect the confidentiality, integrity, and availability of backup information at storage locations.

(j) VA will establish a physical security program to protect VA IT from damage, loss, theft, or unauthorized physical access in accordance with VA policy.

(k) VA will update policies and procedures to address system and organizational changes or problems encountered during implementation, execution, or testing of the VA information security program.

(l) VA will implement a threat awareness program 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) VA will develop, test, implement, manage, and maintain appropriate response and recovery plans. At a minimum, VA will manage and test all plans on a yearly basis, including Incident Response, Business Continuity, Incident Recovery, and Disaster Recovery plans.

(n) VA will develop cybersecurity workforce management policies and capabilities to support identification and qualifications for a professional cybersecurity workforce.

(o) VA personnel may be considered for administrative or judicial sanctions if they knowingly, willfully, or negligently compromise, damage, or place at risk VA information by not ensuring implementation of VA security requirements in accordance with VA policy.

(p) VA will identify, report, and correct system flaws and incorporate flaw remediation into VA's configuration management process.

(5) Media Sanitization

(a) VA will comply with NIST 800-88 for the purposes of media sanitization on all IT equipment.

(b) VA will use approved techniques or methods to dispose of, destroy, or erase VA information, 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.

(c) The VA Office of Inspector General (OIG) may issue a separate, more stringent electronic media sanitization policy, which OIG must follow, due to special security needs or resulting from the need to follow special procedures to ensure the admissibility of electronic evidence in legal proceedings.

(d) VA offices and facilities notified by the Office of the 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 (OI&T) staff must train Information Security Officers (ISOs) (and other designated staff assigned to perform media sanitization and/or process electronic storage media for sanitization) 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) must include the appropriate security language concerning the protection of VA assets, including appropriate media sanitization for electronic storage media and 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 CIO), 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) VA has a contracted, agency-wide program in place to sanitize and properly dispose of media containing VA sensitive information. ISOs are the points of contact for this program and facilitate all phases of the program for each Administration and Staff Office.

(i) IT electronic media may be sanitized under a locally developed contract or in-house, whichever is deemed to be more cost-effective. Procedures for contracting sanitization services or completing services in-house are outlined in this directive and must be followed.

(j) 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 OI&T 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.

(k) When non-VA owned IT equipment is no longer used to access or store VA sensitive information, all equipment hard disk 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.

(l) OI&T and facility property managers are required to report within VA usable excess IT equipment 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.

(m) OI&T 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.

(6) Maintenance

(a) VA will perform maintenance and repairs of VA IT ISs and system components consistent with VA policies and procedures.

(b) VA will schedule, document, manage, and review records of maintenance, repair, or replacements of system components 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) VA will approve and monitor all maintenance activities, 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) VA will manage technical security solutions to ensure the security and resilience of systems and assets are consistent with related policies, procedures, and agreements.

(b) VA will collect and keep audit data 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) VA will employ technical and non-technical safeguards 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) VA will configure systems 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.

(f) 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 events by implementing the appropriate activities to identify the occurrence of a cybersecurity event. Outcome categories within the Detect Function include: Anomalies and Events; Security Continuous Monitoring; and Detection Processes; and associated activities, as described below:

(1) Anomalies and Events

(a) VA will detect anomalous activities in a timely manner and determine the potential impact of events on VA systems and networks.

(b) VA will sense, correlate, and make visible to mission owners and network operators the security posture, from individual device or software objects to aggregated systems of systems.

(c) VA will receive system security alerts, advisories, and directives from external organizations (e.g., US-CERT) on an ongoing basis and generate internal security alerts, advisories, and directives as deemed necessary.

(d) VA will establish baseline configurations for systems and system components, including communications and connectivity-related aspects of systems. Baseline configurations of systems reflect the current enterprise architecture.

(e) VA will monitor systems to detect attacks, indicators of potential attacks, and unauthorized local, network, and remote connections.

(f) VA will track and document cybersecurity and privacy incidents.

(g) VA will implement an incident handling capability for security and privacy incidents that includes preparation, detection and analysis, impact determination, containment, eradication, and recovery.

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

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

(j) 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) VA will monitor information and assets at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

(b) VA will develop a security and privacy continuous monitoring strategy, and implement a security and privacy continuous monitoring program that assesses security and privacy controls and associated risks at a frequency sufficient to support risk-based 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) VA will establish and maintain a continuous monitoring capability as specified in NIST SP 800-137 that provides cohesive collection, transmission, storage, aggregation, and presentation of data that conveys current operational status to affected VA stakeholders.

(d) VA will monitor physical access to the facility where the system resides to detect and respond to physical security incidents.

(e) VA will monitor personnel activity to detect potential cybersecurity events.

(f) VA will implement an insider threat program that includes a cross-discipline insider threat incident handling team. Insider threat programs include controls 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.

(g) VA will implement malicious code protection mechanisms 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 KS.

(h) VA will define acceptable and unacceptable mobile code and mobile code technologies, and establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies. VA will also authorize, monitor, and control the use of mobile code within its systems.

(i) VA will require that providers of external system services comply with organizational security and privacy requirements. VA will monitor security and privacy control compliance by external service providers on an ongoing basis.

(j) VA will establish policy and procedures 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.

(k) VA will identify software programs authorized to execute on the system and employ a deny-all or permit-by-exception policy (whitelisting) to allow the execution of authorized software programs on the system.

(l) VA will detect network services that have not been authorized or approved.

(m) VA will employ automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the system and take actions when unauthorized components are detected.

(n) VA will enforce physical access authorizations and verify individual access authorizations before granting access to the facility to prevent unauthorized personnel from accessing VA facilities and systems.

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

(3) Detection Processes

(a) VA will maintain and test detection processes and procedures to ensure timely and adequate awareness of anomalous events.

(b) VA will require personnel to report suspected security and privacy incidents to the organizational incident response capability.

(c) VA will provide 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.

(d) VA will implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems are developed and 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 event and identifies the appropriate actions to take regarding the detected cybersecurity event. Outcome categories within the Respond Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements; and associated activities, as described below:

(1) Response Planning

(a) VA will develop and implement an incident response plan that provides the organization with a roadmap for implementing its incident response capability. For incidents involving PII/PHI, VA will include a process to determine whether notice to oversight organizations or affected individuals is appropriate and provide that notice accordingly.

(b) VA will execute and maintain response processes and procedures to ensure timely response to detected cybersecurity events.

(2) Communications

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

(b) VA will explicitly designate responsibility for incident response in the Incident Response Plan.

(c) VA will require personnel to report suspected security, privacy, and supply chain incidents.

(d) VA will coordinate among many organizational entities including, for example, mission/business owners, SOs, AOs, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function), to effectively handle incidents.

(e) VA will contact personnel on the alert notification list when an alert or notification is issued. Personnel on the alert notification list can include, for example, system administrators, mission or business owners, SOs, system security officers, or privacy officers.

(f) VA will correlate incident information and individual incident responses 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) VA will conduct analysis to ensure adequate response and support recovery activities.

(b) VA will employ automated tools and mechanisms to support near real-time analysis of alerts and notifications generated by VA systems.

(c) VA will test the incident response capability for the system to determine the incident response effectiveness and document the results.

(d) VA will determine the impact of an incident on VA's mission and business practices.

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

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

(g) VA will 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.

(4) Mitigation

(a) VA will perform activities to prevent expansion of an event, mitigate its effects, and eradicate the incident.

(b) VA will mitigate risk of a security or privacy incident to the 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; in these cases, a POAM will be generated.

(d) VA will incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.

(5) Improvements

(a) VA will improve organizational response activities by incorporating lessons learned from current and previous detection/response activities.

(b) VA will use qualitative and quantitative data from incident response testing and actual events 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) VA will update the Incident Response Plan 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 event. Outcome Categories within the Recover Function include: Recovery Planning; Improvements; and Communications; and associated activities, as described below:

(1) Recovery Planning

(a) VA will define necessary incident recovery plans and will test those plans in accordance with federal guidelines.

(b) VA will execute and maintain recovery processes and procedures to ensure timely restoration of systems or assets affected by cybersecurity events in accordance with disaster recovery plans.

(c) VA will develop and implement contingency plans 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) VA will improve recovery planning and processes by incorporating lessons learned into future activities.

(b) VA will update contingency plans 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) VA will coordinate restoration activities with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other computer security incident response teams, and vendors.

(b) VA will manage communication with the public regarding cybersecurity and privacy incidents through the Office of Public and Intergovernmental Affairs (OP&IA).

(c) VA will manage its reputation after an incident has been resolved through OP&IA.

(d) VA will share information internally on recovery activities among organizational stakeholders, including, for example, executive and management teams, mission/business owners, SOs, 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 carry out the responsibilities under 38 U.S.C. § 5723 and 44 U.S.C. § 3554.

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

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

(2) Charter and co-chairs the cybersecurity governing body.

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

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

(5) Direct and coordinate with the Executive Director for Quality, Performance and Risk (QPR) to ensure that risk management strategies and policies are aligned with overarching VA cybersecurity strategy.

(6) Direct and coordinate with the Deputy Assistant Secretary (DAS) for IT Resource Management (ITRM) to develop cybersecurity workforce management policies and capabilities to support identification and qualifications for a professional cybersecurity workforce.

(7) Direct and coordinate with the Assistant Secretary for the Office of Operations, Security, and Preparedness (OSP) to ensure that cybersecurity 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 for Office of Acquisition and Logistics to ensure that cybersecurity

responsibilities are integrated into processes for VA acquisition programs, including research and development.

(9) Direct and coordinate with the DAS for IT Operations and Services (ITOPS) to ensure that cybersecurity responsibilities are integrated into the operational testing and evaluation for VA programs.

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

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

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

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

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

(15) Appoint an AO for all VA IT systems and ensure all VA systems are authorized.

(16) Appoint a senior employee to chair a committee to provide oversight for VA's selected Governance, Risk and Compliance tool committee.

(17) Ensure an annual assessment of the VA cybersecurity program is conducted.

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

(1) Make authorization decisions for VA ISs under their purview by formally assuming responsibility for operating VA ISs at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

e. **Deputy Chief Information Officer (DCIO) for Office of Information Security (OIS).** Under the authority and direction of the VA CIO, and in addition to the responsibilities as the VA Chief Information Security Officer **(**CISO), the DCIO, OIS shall:

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

(2) Chair the cybersecurity governing body.

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

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

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

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

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

(8) Establish and maintain the VA Information Security KS.

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

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

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

(12) 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.

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

(14) 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).

(15) Implement a process to ensure that POAMs for the security and privacy programs and associated organizational systems are developed and maintained.

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

(1) Direct and coordinate the VA cybersecurity program and, as delegated, carries 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, SOs, and ISOs.

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

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

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

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

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

(8) Coordinate with Executive Director, QPR to ensure cybersecurity 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 KS.

(10) Develop VA IS contingency plans and conducts exercises to recover IS services following an emergency or IS disruption.

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

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

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

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

(15) Develop cybersecurity workforce management policies and capabilities.

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

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

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

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

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

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

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

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

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

(9) 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 ISs supporting those mission and business processes.

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

(11) Advise AOs, CIOs, ISOs, 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, POAMs, risk mitigation approaches, security alerts, and potential adverse effects of identified vulnerabilities.

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

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

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

h. **Deputy Assistant Secretary for IT Operations and Services (ITOPS).** Under the authority and direction of the VA CIO, the DAS, 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.

i. **Deputy Assistant Secretary for IT Resource Management (ITRM).** The DAS, ITRM shall:

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

(2) Monitor and oversee all VA IT investments.

(3) 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.

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

j. **Cyber Security Operations Center** (CSOC). The VA CSOC shall:

(1) Coordinate among many organizational entities to effectively handle incidents and ensure correlation of incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

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

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

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

(5) Conduct forensic activities as defined in the VA Cybersecurity Incident Response Plan.

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

(7) 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.

k. **Executive Director for Quality, Performance and Risk (QPR).** The Executive Director, QPR shall:

(1) Align cybersecurity strategies, policies, and capabilities with overarching VA cyberspace policy, and supports policies and capabilities relating to the disclosure of sensitive information.

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

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

l. **Under Secretaries, Assistant Secretaries, and Other Key Officials.** The 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.

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

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

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

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

(7) 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.

(8) Ensure that personnel occupying cybersecurity 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.

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

(10) Ensure that cybersecurity 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.

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

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

(13) Implement cybersecurity capabilities responsive to VA requirements.

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

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

(1) Coordinate with the VA CIO on development and implementation of cybersecurity 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.

n. **VA Assistant Secretary for Enterprise Integration**. The VA Assistant Secretary for Enterprise Integration shall:

(1) Establish and co-chair a Data Governance Council that coordinates across VA, facilities 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 organizational Computer Matching Agreements.

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

(4) Coordinate with OI&T to ensure that the enterprise level cybersecurity 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. **VA Senior Agency Official for Privacy (SAOP).** The VA SAOP shall:

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

(2) Oversee, coordinate, and facilitate 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: (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 ISs.

p. **VA IT System Owners (SOs) and/or Technical Data Stewards.** The VA IT SOs and 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 component of the VA Enterprise Architecture and to make maximum use of enterprise cybersecurity.

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

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

q. **Information Security Officers (ISOs).** The ISOs shall:

(1) Implement and enforce all cybersecurity policies and procedures on all VA ISs.

(2) Ensure that all users are informed of their cybersecurity responsibilities for VA ISs under their purview before being granted access to those systems.

(3) Develop incident communication reports when a cybersecurity incident or vulnerability is discovered, and ensure that a process is in place for authorized users to report all cybersecurity events and potential threats and vulnerabilities.

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

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

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

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

(2) Notify the responsible ISO of any changes that might affect security posture.

(3) Comply with the responsibilities of 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) 44 U.S.C. § 3554, *Federal Agency Responsibilities*

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

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

(2) FIPS 140-2, *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) Special Publications (SP)

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

(2) National Institute of Standards and Technology Special Publication 800-34, *Contingency Planning Guide for Federal Information Systems*

(3) National Institute of Standards and Technology Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*

(4) National Institute of Standards and Technology Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*

(5) National Institute of Standards and Technology Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*

(6) National Institute of Standards and Technology Special Publication 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*

(7) National Institute of Standards and Technology Special Publication 800-88, *Guidelines for Media Sanitization*

(8) National Institute of Standards and Technology Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*

(9) National Institute of Standards and Technology Special Publication 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*

(10) National Institute of Standards and Technology Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*

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

(1) OMB Circular A-19, *Legislative Coordination and Clearance*

(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*

**e. VA Policy**

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

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

## 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: SP 800-37

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

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

d. **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 ISOs. SOURCE: SP 800-53

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

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

g. **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. Controlled Unclassified Information may also be referred to as VA Sensitive Information. SOURCE: 32 C.F.R. Part 2002 and NIST SP 800-171

h. **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

i. **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 COS on May 19, 2017

j. **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

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

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

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

n. **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 information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. SOURCE: SP 800-53

o. **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.

p. **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

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

r. **Knowledge Service (KS)**: VA's knowledge portal for providing cybersecurity policies, procedures, and guidance.

s. **Mission Owner**: Those leaders responsible for delivering day-in and day-out VA care services and products to Veterans, meeting their goal for improving customer experience. SOURCE: VA Functional Organization Manual v3.1

t. **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.

u. **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: SP 800-53

v. **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: SP 800-53

w. **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: SP 800-34

x. **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

y. **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: SP 800-53

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

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

bb. **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

cc. **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: SP 800-37

dd. **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: SP 800-53

ee. **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

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

gg. **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

hh. **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: SP 800-34

ii. **System Owner (SO)**: 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

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

kk. **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 also be referred to as Controlled Unclassified Information (CUI).

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

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