UPDATE TO VA DIRECTIVE 6500 VA CYBERSECURITY PROGRAM

1. **PURPOSE:** This notice revises the policy in Department of Veterans Affairs (VA) Directive 6500 to address new security requirements.

2. **POLICY:**

   a. VA Directive 6500 is hereby amended as follows:

      (1) Page 3, section 2: Replace “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” with “VA will use security and privacy controls as defined in NIST SP 800-53 and will follow the security and privacy control baselines in CNSSI No. 1253.”.

      (2) Page 6, section 2.a.(4)(a): Replace “An understanding of the cybersecurity and privacy risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals must be demonstrated” with “VA uses risk assessments to identify the unique risks affecting an environment's mission, functions, image, reputation, organizational assets, and stakeholders to tailor assessment objectives and protections implemented within the environment.”.

      (3) Page 6, section 2.a.(4)(b): Replace “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” with “Risk assessments must be performed in accordance with NIST SP 800-30.”.

      (4) Page 6, section 2.a.(4)(c): Replace “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” with “Risk Assessments are reviewed and updated in accordance with the frequency defined within the Security Control Explorer.”.

      (5) Page 6, section 2.a.(4)(d): Replace “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”

with “Risk Assessments are documented within VA's Governance Risk and Compliance (GRC) tool.”.

(6) Page 7, section 2.a.(4)(e): Move “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.” to section 2.b.(2)(f).

(7) Page 7, section 2.a.(4)(f): Move “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.” to section 2.a.(5)(i).

(8) Page 7, section 2.a.(4)(g): Move “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.” to section 2.d.(4)(e).

(9) Page 7, section 2.a.(4)(h): Move “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.” to section 2.d.(4)(f).

(10) Page 7, section 2.a.(4)(i): Move “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.” to section 2.a.(1)(f).

(11) Page 10, section 2.b.(3)(h): Replace “VA will employ integrity verification tools to detect unauthorized changes to selected software, firmware, hardware, and information” with “VA will approve and employ integrity verification tools to detect unauthorized changes to selected software, firmware, hardware, and information.”

(12) Page 10, section 2.b.(4)(c): Replace “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" with "When technically feasible, automation shall be used 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."

(13) Page 16, section 2.c.(2)(h): Replace "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" with "Malicious code protection mechanisms will be implemented at system entry and exit points to detect and eradicate malicious code. Code protection mechanisms will be updated whenever new releases are available."

(14) Pages 16, section 2.c.(2)(l): Replace "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" with "Through VA's Technical Reference Model (TRM), 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. Information Systems will utilize VA approved software that is in compliance with applicable copyright laws and software license agreements.".

(15) Page 16, section 2.c.(2)(n): Replace "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" with "When technically feasible, automated mechanisms must be employed to detect the presence of unauthorized hardware, software, and firmware components within the system. When unauthorized components are detected, the automated mechanisms will take action.".

(16) Page 18, section 2.d.(3)(b): Replace "Automated tools and mechanisms must be employed to support near real-time analysis of alerts and notifications generated by VA Information Systems" with "When technically feasible, automated tools and mechanisms must be employed to support near real-time analysis of alerts and notifications generated by VA Information Systems.".

3. **RESPONSIBLE OFFICE:** Office of Information and Technology (OIT) (005); Office of Information Security (005R).

4. **RELATED HANDBOOK:** VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program, February 24, 2021.

5. **RESCISSION:** This notice will be rescinded, and the policy above will be incorporated into VA Directive 6500 no later than one year after the date of publication.

CERTIFIED BY:

/s/
Guy T. Kiyokawa
Assistant Secretary for
Enterprise Integration

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
Kurt D. DelBene
Assistant Secretary for
Information and Technology
and Chief Information Officer

DISTRIBUTION: Electronic Only