UPDATE TO VA HANDBOOK 6500 RISK MANAGEMENT FRAMEWORK FOR VA INFORMATION SYSTEMS VA INFORMATION SECURITY PROGRAM

1. **PURPOSE.** This notice revises the policy in the Department of Veterans Affairs (VA) Handbook 6500 to address new security requirements as described below.

2. **POLICY.**

   a. VA Handbook 6500 is hereby amended as follows:

      (1) Page 10, section 4(2)(e): Replace “Ensure that security controls and assessment procedures used by VA are consistent with control correlation identifiers (CCIs), security requirements guides, security technical implementation guides (STIGs), and NIST;” with “Ensure that security and privacy controls and assessment procedures used are consistent with VA policy, NIST standards and system specific control requirements;”.

      (2) Page 13, section 4.c.(10)(e): Remove “Develop and manage automation requirements for VA services that support the RMF; and “.

      (3) Page 17, section 4(13)(c): Replace “Monitor and tracking overall execution of CCI-level POA&M;” with “Monitor and track overall execution of POA&Ms;”.

      (4) Page 17-18, section 4(15)(d): Replace “Assist in the overall development, maintenance, and tracking of the security plan for assigned information system and platform IT systems, to include identification of applicable CCIs (Common security controls owner performs this function for inherited controls.);” with “Lead the overall development, maintenance, and tracking of the security plan for assigned information system and platform IT systems, to include identification of applicable controls;”.

      (5) Page 19, section 4.c.(17)(c): Replace “In coordination with the Information System Owner, ISSO and other Privacy Services Office stakeholders, assess and submit a Privacy Impact Assessment (PIA) and Privacy Threshold Analysis (PTA) when required.” with “In coordination with the Information System Owner, ISSO and other VA Privacy Service stakeholders, complete and submit a Privacy Threshold Analysis (PTA) to identify the type of data residing in the information system. If personally identifiable information (PII) resides in the information system, determine if a Privacy Impact Assessment (PIA) is required, whether a System of Records Notice is required, and if any other privacy requirements apply to the information system. If a PIA, SORN, or other privacy requirements are required, coordinate with applicable parties (e.g., VA Privacy Service and Administration-level Privacy Offices) to ensure compliance and manage risks with respect to privacy. Develop and submit the PIA to VA Privacy Service for approval.”.

(6) Page 20, section 4.(19)(a): Replace “Conduct an onsite assessment of the security controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., to determine if the documented controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements identified for protecting the system at its specified level of sensitivity);” with “Conduct an assessment of the security and privacy controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., to determine if the documented controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements identified for protecting the system at its specified level of sensitivity);”.

(7) Page 20, section 4.(19)(b): Replace “Provide an assessment of the severity of weaknesses or deficiencies discovered in the information system and its environment of operation through the onsite assessment and recommend corrective actions to address identified vulnerabilities;” with “Provide an assessment of the severity of weaknesses or deficiencies discovered in the information system and its environment of operation through the assessment and recommend corrective actions to address identified vulnerabilities;”.

(8) Page 21, section 5,a.(1): Remove “STIGs are associated with security controls through CCIs, which are decompositions of NIST SP 800-53 security controls into single, actionable, measurable items.”.

(9) Page 26-27, section 6.b.(5)(a)ii: Remove “CCIs are designed to be “inherited” by information systems and can be designated as a combination of common and system-specific controls, known as a hybrid control.”.

(10) Page 29, section 6.b.(5)(c)vii.a: Replace “When this becomes necessary, CCIs from CNSSI 1253 should be considered first.” with “When this becomes necessary, control statements from CNSSI 1253 should be considered first.”.

(11) Page 31, section 6.b.(5)(c)viii.g.: Remove “Security control support by automated mechanism is only required where they are available and feasible.”.

(12) Page 32, section 6.b.(5)(e): Remove “The strategy must include the plan for annual assessments of a subset of implemented security controls, and the level of independence required of the assessor. The breadth, depth, and rigor of these annual assessments should be reflective of the security categorization of the system and threats to the system.”.

(13) Page 34, section 6.b.(7)(c): Replace “POA&Ms are developed as part of the security authorization package, along with any artifacts produced during the assessment (e.g., output from automated test tools or screen shots that depict aspects of system configuration).” with “POA&Ms are developed as part of the security authorization package, along with any artifacts produced during the assessment (e.g., output from test tools or screen shots that depict aspects of system configuration).”.

(14) Page 35, section 6.b.(7)(d)iv: Replace “Vulnerability severity values for security controls are informed by assessment at the CCI level. If a control has a STIG or Security Requirements Guide associated through CCIs, the vulnerabilities identified by STIG or Security Requirements Guide assessments will be used to inform the overall vulnerability severity value for the security control.” with “Vulnerability severity values are assigned to all non-compliant controls as part of the security control analysis to indicate the severity associated with the identified vulnerability.”.

(15) Page 45, section 6.b.(8)(i)i.: Replace “Assessment information produced by an assessor during continuous monitoring is provided to the System Owner and the common control provider in updated assessment reports or via reports from automated security/privacy management and reporting tools.” with “Assessment information produced by an assessor during continuous monitoring is provided to the System Owner and the common control provider in updated assessment reports or via reports from security/privacy management and reporting tools.”.

(16) Page 45, section 6.b.(8)(i)iv.: Replace “Recommendations for remediation actions may also be provided by an automated security/privacy management and reporting tool.” with “Recommendations for remediation actions may also be provided by a management and reporting tool.”.

(17) Page 46, section 6.b.(8)(m): Replace “Review the security and privacy posture of the system on an ongoing basis, as needed, at least annually or when a major change to the system occurs, to determine whether the risk remains acceptable.” with “Review the security and privacy posture of the system in accordance with the frequency defined within the Security Control Explorer.”.

(18) Page 46, section 6.b.(9)(a): Replace “The results of an annual review or a major change in the cybersecurity posture at any time may indicate the need for reassessment and reauthorization of the system.” with “Identified weaknesses or the results of a major change in the cybersecurity posture at any time may indicate the need for reassessment and reauthorization of the system.”.

(19) Page A-1, appendix A.9: Remove definition, “Control Correlation Identifier (CCI): Allows a high-level statement in a policy document to be ‘decomposed’ and explicitly associated with the low-level security settings that must be assessed to determine compliance with the objectives of that specific statement. SOURCE: NIST SP 800-53, CNSSI 4009”.

(20) Page B-1, appendix B.56: Remove acronym/abbreviation for “CCI”.

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

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

5. **RESCISSION(S).** This notice will be rescinded, and the policy above will be incorporated into VA Handbook 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