Department of Veterans Affairs

Memorandum

Date:

From: Assistant Secretary for Information and Technology and Chief Information Officer (005)

Subj: VA Critical Security Controls

To: Under Secretaries, Assistant Secretaries and Other Key Officials

Thru: Deputy Assistant Secretary for Information Security & Chief Information Security Officer (005R)

1. Due to the continually evolving cyber security risks to federal and VA information systems there is a need for VA Chief Information Officer (CIO) to establish minimum mandatory security requirements for all new systems and applications. Implementing *VA's Critical Security Controls* (Appendix A) will enable VA to elevate our cyber security posture in an effort to mitigate the ongoing threats to VA's mission. Effective July 1, 2025, any network connected software system or service must have the *VA Critical Security Controls* implemented prior to being authorized for use in the VA.

2. Critical Security Controls are intended to increase VA's security posture and provide security and privacy risk visibility into the VA network and is not a new requirement. The functional requirement is not negotiable and Plan of Action & Milestones (POAM) will not be accepted in the event these controls cannot be implemented for new systems. Failure to maintain these VA Critical Controls after implementation shall result in VA discontinuing the use of the system.

3. The escalating cyber threats, coupled with the digitization of healthcare and increasingly interconnected systems, demands urgent attention to cyber security. Patient safety, regulatory compliance, financial stability, and public trust are all at risk. It's imperative that the VA prioritize robust cybersecurity measures to safeguard these critical areas. Critical Security Controls will enable VA CIO, CISO and Business Owner(s) to ensure the secure operation of VA systems. Further questions related to this memorandum can be directed to Amber Pearson, amber.pearson3@va.gov (540) 455-8050.

Kurt D. DelBene

Attachment: VA Critical Security Controls Frequently Asked Questions (FAQ)

KURT DELBENE

Digitally signed by KURT DELBENE
Date: 2025.01.17 11:29:13 -08'00'

Signature block of Approving Official

Date

Appendix A – VA Critical Security Controls

Mandatory Requirement	NIST Associated Control(s)	NIST Control Title	Purpose / Intent
Enforce Multi-Factor Authentication (MFA) for all systems.	IA-2(1)	MFA to Privileged Accounts	Zero Trust/MFA
	IA-2(2)	MFA to Non-Privileged Accounts	Zero Trust/MFA
Explicitly authenticate, authorize, and disable all subjects, assets, and workflows across systems.	AC-2	Access Management	Zero Trust/Access Control
Restrict data access with the principle of least privilege and least functionality.	AC-5, AC-6	Least Privilege	Zero Trust/Access Control
Ensure all system assets are logged, inventoried, and scanned by VA's Cybersecurity Operations Center (CSOC).	CM-8	System Component Inventory	Zero Trust/Asset Management
Ensure CSOC has visibility and logging for continuous monitoring of the system, network, physical environment, cloud services, connections, and personnel activity.	AU-2	Event Logging	Zero Trust/ Logging/Monitoring
	SI-4	System Monitoring	Zero Trust/Asset Management, Monitoring
	AU-6	Audit Record Review, Analysis, and Reporting	Zero Trust/ Logging/Monitoring
Ensure system follows VA's enterprise vulnerability management process to track, analyze, and respond to vulnerabilities.	RA-5	Vulnerability Monitoring/Scanning	Zero Trust/Monitoring
	SC-7	Boundary Protection	Zero Trust/Secure Network Connections
	CM-7	Least Functionality	Access Control
Encrypt all Data at Rest (DAR) and Data in Transit (DIT) in accordance with Federal Information Processing (FIPS) 140-2 (or its successor)	SC-28	Protection Of Information at Rest	Zero Trust/Information/Data Protection
	SC-8	Transmission Confidentiality and Integrity	Zero Trust/Information/Data Protection
	CA-3	Information Exchange	Zero Trust/Secure Network Connections
Ensure contingency and incident response plans are assessed and tested in accordance with system categorization requirements.	CP-4	Contingency Plan Testing	Zero Trust/Enterprise/System Resiliency
	IR-3	Incident Response Testing	Zero Trust/ Enterprise/System Resiliency
Ensure that sensitive data handling conforms to applicable privacy requirements, determine the privacy risks associated with an information system or activity and evaluate ways to mitigate privacy risks.	NIST SP 800-53 Rev. 4: AR-2 Rev. 5: RA-8	Privacy Impact and Risk Assessment	Zero Trust/Risk Assessment and Management *Note: All Systems require a Privacy Threshold Analysis (PTA); Only Systems processing sensitive data require a PIA*

VA Critical Security Controls Frequently Asked Questions (FAQ)

1. **What are the VA Critical Security Controls?**

   The VA CIO has established the VA Critical Security Controls as the minimum mandatory requirements for all new network connected VA systems and applications in the memorandum titled "VA Critical Security Controls". These controls support progressing VA's Zero Trust First Cyber Security Strategy, while strengthening the security posture of our digital infrastructure. These objectives and controls incorporate the CIO's key security concerns, Zero Trust First Cyber Security Strategy goals, Cybersecurity Operations Center (CSOC) recommendations, and other OIS identified security gaps. The VA Critical Security Controls may change based on VA strategic initiatives, OIS/OIT organizational maturity, and emerging Federal requirements.

2. **Who is the intended audience of the VA Critical Security Controls memorandum?**

   The VA Critical Security Controls memorandum is intended for all VA personnel with information system and application security responsibilities such as Authorizing Officials, Information System Owners, Information System Security Officers, and other key system stakeholders.

3. **Does the VA Critical Security Controls memorandum apply to all systems within the Veterans Affairs (VA), including all three branches, Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), and National Cemetery Administration (NCA)?**

   Yes. The CIO and Chief Information Security Officer (CISO) have delegated responsibilities under the Federal Information Security Modernization Act (FISMA) including ensuring the agency's information systems compliance with security requirements as defined by FISMA and the guidance provided by the National Institute of Standards and Technology (NIST) Special Publication 800-53. The intent of the memorandum is to clearly articulate the CIO and CISO enforcement of system compliance with our most critical security controls during the authorization to operate (ATO) process for all VA systems including VHA, VBA and NCA systems.

4. **When must the VA Critical Security Controls be implemented on <u>new</u> systems?**

New information systems, applications, and specialized devices (medical devices/systems, special-purpose systems, and research scientific computing devices) seeking ATO must comply with the minimum mandatory requirements of the VA Critical Security Controls by **July 1, 2025**. Plan of Action and Milestones (POA&M) will not be accepted in the event these controls cannot be implemented for new systems.

5. **When must the VA Critical Security Controls be implemented on existing systems?**

   Existing systems must also implement these mandatory requirements. If a critical security control cannot be implemented, a POA&M must be created by **July 1, 2025**. POA&Ms related to the VA Critical Security Controls will be regularly monitored by OIS.

6. **Will the VA Critical Security Controls apply regardless of the system's categorization level?**

   Yes, the critical controls must be implemented for all system categorization levels (Low, Moderate, and High).

7. **What if the specialized device I'm deploying cannot implement a Critical Security Control due to technical limitations?**

   Newly procured medical and special purpose devices must comply with the VA Critical Security Controls. If an existing medical and special purpose devices cannot meet the requirements of certain VA Critical Security Controls due to a technical limitation and all mitigation options have been exhausted, the System Owner in collaboration with the ISSO, must submit a Risk Acceptance Request in accordance with the POA&M Management Guide – Risk Acceptance Approval process. Only a VA Authorizing Official may approve a Risk Accepted POA&M and accept the risk associated with the specialized device.

8. **How will VA Critical Security Controls be identified in eMASS?**

   The VA Critical Security Controls will be labeled as "VA Critical Security Controls" in the Control Policy Volumes on Knowledge Service, as well as in VA's Governance, Risk, and Compliance (GRC) tool, Enterprise Mission Assurance Support Service (eMASS). Communications will be sent to system stakeholders when changes are made to the VA Critical Security Controls listing.

9. **How often will these controls be reviewed in eMASS?**

   The VA Critical Security Controls will be reviewed as part of the standard ATO process (e.g., during Risk Management Framework [RMF] Step 4, Security Controls Assessments [SCAs]) and as part of Continuous Monitoring processes.

10. **How will the VA Critical Security Controls memorandum affect remote users including those in the community connected to a VA-issued hotspot device or those who telework?**

    Most users will not see a difference in their daily operations. These critical controls are meant to ensure that VA is using the highest security standards when authorizing systems to operate on the VA network.

11. **If the control is inherited from another system how does that impact my system?**

    If the non-compliant VA Critical Security Control is inherited, the system providing the control (parent system) must develop a POA&M to resolve the issue. OIS will work with enterprise control providers to ensure system inheritance of the controls is well documented.

12. **What is the process if the VA Critical Security Control(s) fail for the system?**

    In the event of security control failure, Authorizing Officials (AOs) shall follow the established risk escalation process prior to an authorization decision.

13. **Do VA Critical Security Controls apply to assess only packages in eMASS?**

    The VA Critical Security Controls, as applicable in the current VA Assess-only baseline per Appendix B of the Assess Only Requirements SOP, will be the only critical controls assessed per the memorandum. Assess Only systems are associated with a supporting platform, enclave, or information system (i.e., parent system)– which will have an ATO. The complete list of critical controls compliance will be assessed during the assessment and authorization process of the parent system.

14. **Will VA Critical Security Controls be required to be included in VA Contracts and Acquisitions for contractors, subcontractors, or third-party servicers and associates to comply with?**

Yes, VA plans to mandate the inclusion of VA Critical Security Controls in solicitations and contracts through updates to VA Handbook 6500.6, Appendix C, to ensure that all contractors and vendors comply with applicable VA security standards.

15. **Are technologies researched, developed, and transferred to the nonfederal sector through Cooperative Research and Development Agreements (CRADAs) subject to compliance with the VA Critical Security Controls?**

    Yes, VA Critical Security Controls are mandatory security requirements for all new systems and applications at VA. If the technology in question is a medical or special purpose device, please see Question 7 for additional details.