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

Page 2:

VA Critical Security Controls

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*