DEPARTMENT OF THE ARMY
CHIEF INFORMATION OFFICER
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

CS-SEC-RI-053

SAIS-CS (25-1rrrr)

21 November 2024

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Risk Management Framework Modernization

1. References.

a. AR 25-2 (Army Cybersecurity)

b. DCS, G-6 memorandum (Amplifying Guidance Regarding the Implementation of Army Cybersecurity Reform, Army Risk Management Framework (formally Risk Management Framework (RMF) 2.0)), 12 September 2023

c. U.S. Army NETCOM memorandum (Operational Tactics, Techniques, and Procedures (Risk Management Framework (formally RMF 2.0)), 24 February 2024

2. Purpose. To provide updates and direction to the Army Risk Management Framework (RMF) Modernization effort.

3. Background.

a. Current State. Per reference 1b, RMF development and execution focuses on operationalizing the process by prioritizing threat-based controls, taking advantage of inheritance, providing tools for automation of labor-intensive tasks to streamline assessments, and setting the foundation for systems to enter Continuous Monitoring (ConMon). Despite the implementation of RMF, challenges remain with efficiency and addressing the continuous evolving Intel-based threats posing real risks to the Army terrain.

b. Way Forward. The foundation to the framework must be reset and reinforced to support cyber hygiene across the DoDIN-A, while effectively measuring and mitigating risk against evolving threats. The enclosed Plan of Action and Milestones (POA&M) product (Enclosure 1), identifying critical changes, training opportunities, and policy updates to address the ever-changing cyber environment. This is a necessary fundamental cultural shift to force shared understanding, acceptance, and risk taking. Capabilities are being delivered expeditiously to the Army through development, security, and operation (DSO) pipelines and with a durable foundation, risk base decision making is decentralized and competitive with the pace of change. This will support the approach on how to best leverage capabilities and protect the resources.

4. Direction.

a. There will be a singular Control Assessor (CA) assessment. Thus, the multiplicity of CA assessments is eliminated. OCIO will update AR 25-2 and remove additional control assessment designations.

b. This memorandum removes the Army-wide deadline for systems to enter Continuous Monitoring as directed in reference 1b. Authorizing Officials will work with System Owners to determine appropriate timelines to enter Continuous Monitoring.

c. Update the Critical Security Controls Listing to reflect 52 vs 40 controls and enhancements (Enclosure 2). This is to include both Access Control (AC) and Audit (AU) listings. Controls were removed from the Security Assessment & Authorization (CA) and the Contingency Planning (CP). Controls were modified from the Identified & Authentication (IA) and Incident Response (IR) listings.

5. This memorandum is effective immediately and will stay in effect until rescinded.

6. Points of contact.

a. CIO Policy Inbox: usarmy.pentagon.hqda-cio.mbx.policy-inbox@army.mil

b. CIO RMF Inbox: usarmy.pentagon.hqda-cio-g-6.mbx.rmf-team@army.mil

c. SAIS-CS: Ms. Suzanne Rodriguez, suzanne.p.rodriguez.civ@army.mil

GARCIGA.LEONEL.T.1186170411
Digitally signed by GARCIGA.LEONEL.T.1186170411
Date: 2024.11.21 16:04:43 -05'00'

Encls

LEONEL T. GARCIGA
Chief Information Officer

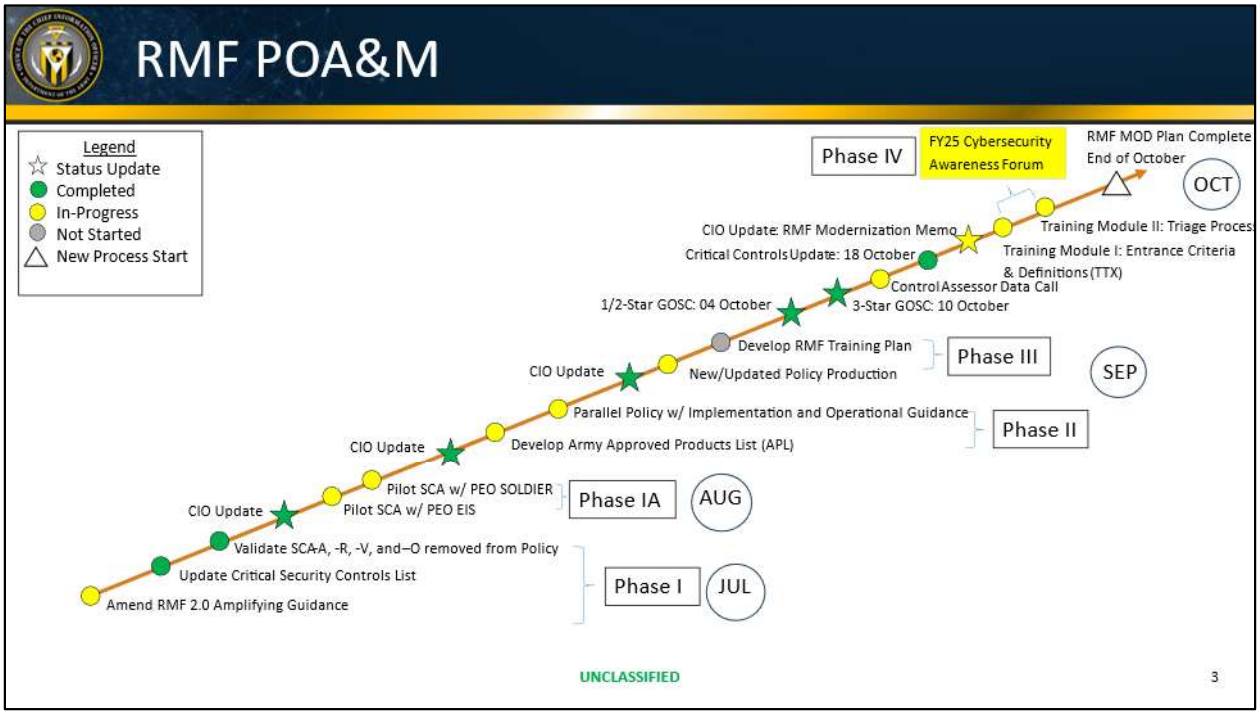
DISTRIBUTION:
Principal Officials of Headquarters, Department of the Army
Commander
U.S. Army Forces Command
U.S. Army Training and Doctrine Command
U.S. Army Materiel Command
U.S. Army Futures Command
U.S. Army Pacific
(CONT)

DISTRIBUTION: (CONT)
- U.S. Army Europe and Africa
- U.S. Army Central
- U.S. Army North
- U.S. Army South
- U.S. Army Special Operations Command
- Military Surface Deployment and Distribution Command
- U.S. Army Space and Missile Defense Command/Army Strategic Command
- U.S. Army Cyber Command
- U.S. Army Medical Command
- U.S. Army Intelligence and Security Command
- U.S. Army Corps of Engineers
- U.S. Army Military District of Washington
- U.S. Army Test and Evaluation Command
- U.S. Army Human Resources Command
- U.S. Army Corrections Command

Superintendent, U.S. Military Academy
Commandant, U.S. Army War College
Director, U.S. Army Civilian Human Resources Agency
Executive Director, Military Postal Service Agency
Director, U.S. Army Criminal Investigation Division
Director, Civilian Protection Center of Excellence
Superintendent, Arlington National Cemetery
Director, U.S. Army Acquisition Support Center

CF:
Principal Cyber Advisor
Director of Enterprise Management
Director, Office of Analytics Integration
Commander, Eighth Army

Plan of Action & Milestones



ENCLOSURE 1

Critical Security Controls

Control	Name
AC-2	Account Management
AC-3	Access Enforcement
AC-4	Information Flow Enforcement
AC-5	Separation Of Duties
AC-6	Least Privilege
AC-6 (9)	Least Privilege | Auditing Use Of Privileged Functions
AC-7	Unsuccessful Logon Attempts
AC-9	Previous Logon (Access) Notification
AC-10	Concurrent Session Control
AC-11	Session Lock
AC-12	Session Termination
AC-17	Remote Access
AC-17 (2)	Remote Access | Protection Of Confidentiality / Integrity Using Encryption
AC-18	Wireless Access
AC-19	Access Control For Mobile Devices
AC-20	Use Of External Information Systems
AC-24	Access Control Decisions
AC-25	Reference Monitor
AU-3	Content Of Audit Records
AU-4	Audit Storage Capacity
AU-5	Response To Audit Processing Failures
AU-6	Audit Review, Analysis, And Reporting
AU-9	Protection Of Audit Information
AU-10	Non-Repudiation
AU-13	Monitoring For Information Disclosure
AU-14	Session Audit
AU-16	Cross-Organizational Auditing
CM-6	Configuration Settings
CM-7	Least Functionality
CM-7(1)	Least Functionality | Periodic Review
CM-8	Information System Component Inventory
CM-10	Software Usage Restrictions
IA-2 (1)	Identification And Authentication | Network Access To Privileged Accounts
IA-2 (2)	Identification And Authentication | Network Access To Non-Privileged Accounts
IA-2 (3)	Identification And Authentication | Local Access To Privileged Accounts
IA-2 (4)	Identification And Authentication | Local Access To Non-Privileged Accounts

IA-5	Authenticator Management
IA-5 (1)	Authenticator Management | Password-Based Authentication
IR-6	Incident Reporting
IR-8	Incident Response Plan
IR-9	Information Spillage Response
PL-8	Information Security Architecture
RA-5	Vulnerability Scanning
SA-22	Unsupported System Components
SC-7	Boundary Protection
SC-8	Transmission Confidentiality And Integrity
SC-28	Protection Of Information At Rest
SI-2	Flaw Remediation
SI-3	Malicious Code Protection
SI-4	Information System Monitoring
SI-4 (4)	Information System Monitoring | Inbound And Outbound Communications Traffic
SI-4 (5)	Information System Monitoring | System-Generated Alerts