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

PRP-GOV-CP-031

SAIS-PRP (25-1rrrr) 26 June 2024

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Denial of Authorization to Operate for Internal Controls Over Financial Reporting Systems that fail Cyber Audit Inspections

1. References.

a. AR 25-1 (Army Information Technology).

b. AR 25-2 (Army Cybersecurity).

c. NIST Special Publication 800-53 (Security and Privacy Controls for Information Systems and Organizations).

d. DoDI 8510.01 (Risk Management Framework for DoD Systems).

e. HQDA CIO memorandum (Business System Log Data Ingest to Army Enterprise Unified Security Information and Event Management and Gabriel Nimbus), 17 Nov 2023.

2. Purpose. Due to continued financial audit findings on weak cybersecurity control implementation and continued cybersecurity threat, the Army is prioritizing specific cybersecurity controls for focused implementation. Consistent with authorities and direction in above references, this memorandum identifies the priority controls for Internal Controls over Financial Reporting (ICOFR) systems, specifies immediate consequences of failing to meet these controls, and required remediation approval process.

3. Background. The Army financial audit has reported Notices of Findings and Recommendations (NFRs) concerning critical cybersecurity control in Army ICOFR systems. Several of these findings have been repeated over multiple audit inspections. System owners and Authorizing Officials have taken remedial action to improve the Army's cybersecurity posture. However, cybersecurity in the Army's critical financial systems is a no-fail mission. Therefore, the Army will more actively inspect the Army's priority ICOFR systems against priority controls. Additionally, the Department is

changing its risk tolerance against cybersecurity and failing systems are being taken off-line until remedied.

4. Guidance.

a. Financial Management (FM) Information System Owners and Authorizing Officials (AOs) will implement the 44 critical controls (see enclosure) as a priority, as well as the full RMF system control set based on the baseline categorization and applicable FM overlay.

(1) To obtain and maintain an Authorization to Operate (ATO), systems must implement the minimum control set in the enclosure. Discrepancies in roles and responsibilities or shifting blame to another party allegedly responsible for maintaining an acceptable operational security posture is intolerable. System owners and their service providers must comply with the Risk Management Framework (RMF) and ensure clear roles and responsibilities are defined for controls performance and monitoring in a Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), Service Level Agreement (SLA), and/or Standard Operating Procedures (SOP). System owners will be held responsible failing to do so. A failed inspection will result in a DATO.

(2) This does not negate the need to implement the broader control as part of the RMF.

(3) If a system fails inspection, the CIO will issue a DATO. The CIO will lift the DATO when the system Authorizing Official in coordination with the Network Authorizing Official has provided a detailed way ahead to comply with controls directly to the CIO.

b. Additionally, CIO will mobilize inspection teams to visit each organization using ICOFR Systems with a one-to-two-week notice and verify compliance where possible.

5. Intent. The purpose of this guidance is to mitigate the risk of financial crimes stemming from an insider threat or exploitation of a system vulnerability. By implementing the specified critical controls, organizations strive to protect their ICOFR Systems from unauthorized access and misuse.

6. Points of Contact.

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

b. Mr. Harsh Patel, OCIO Policy Division, harsh.m.patel2.civ@army.mil, (703) 614-8053.

b. Mr. Joe Bryant, OCIO Oversight and Compliance Division Chief, joe.d.bryant4.civ@army.mil, (703) 697-8355.

GARCIGA.LEO
NEL.T.118617
0411

Digitally signed by
GARCIGA.LEONEL.T.11
86170411
Date: 2024.06.26
16:18:04 -04'00'

Encl

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
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
U.S. Army Recruiting 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
(CONT)

DISTRIBUTION: (CONT)
Director, U.S. Army Criminal Investigation Division
Director, Civilian Protection Center of Excellence
Director, U.S. Army Joint Counter-Small Unmanned Aircraft Systems Office
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

CRITICAL SECURITY CONTROLS

It is imperative that systems meet or exceed the standards set forth in the Critical Security Controls criteria. The list below outlines the controls that systems will be inspected on to remain active and have an ATO.

#	Control	Description
1	AC-1	Access Controls Policies and Procedures
2	AC-2	Account Management
3	AC-2(2)	Account Management /Removal of Temporary / Emergency Accounts
4	AC-2(3)	Account Management /Disable Inactive Accounts
5	AC-3	Access Enforcement
6	AC-5	Segregation of Duties
7	AC-6	Lease Privilege
8	AC-6(5)	Least Privilege/Privileged Accounts
9	AC-6(9)	Least Privilege/Auditing Use of Privilege Functions
10	AC-9	Previous Logon (Access) Notification
11	AC-16	Security Attributes
12	AC-21	Information Sharing
13	AU-1	Audit and Accountability Policies and Procedures
14	AU-2	Audit Events
15	AU-3	Content of Audit Records
16	AU-6	Audit Review, Analysis, and Reporting
17	AU-9	Protection of Audit Information
18	AU-12	Audit Generation
19	AT-2	Security Awareness
20	AT-2(2)	Security Awareness/Insider Threat
21	CA-2	Security Assessments
22	CA-2(2)	Security Assessments/Specialized Assessments
23	CA-5	Plan of Action and Milestones
24	CM-1	Configuration Management Policy
25	CM-2	Baseline Configuration
26	CM-2(6)	Baseline Configuration/Development and Test Environments
27	CM-3	Configuration Change Control
28	CM-5	Access Restrictions for Change
29	CP-2	Contingency Plan
30	CP-2(1)	Contingency Plan/Coordinate with Related Plans
31	CP-9	Information System Backup

32	IA-2	Identification and Authentication (Organizational Users)
33	IA-5	Authenticator Management
34	IR-1	Incident Response Policy and Procedures
35	IR-4	Incident Handling
36	IR-4(6)	Incident Handling/Insider Threats-Specific Capabilities
37	IR-4(7)	Incident Handling/Insider Threats-Intra-Organization Coordination
38	PM-10	Security Authorization Process
39	PM-12	Insider Threat Program
40	RA-5	Vulnerability Scanning
41	SI-2	Flaw Remediation
42	SI-4	Information System Monitoring
43	SI-4(12)	Information System Monitoring/Automated Alerts
44	SI-11	Error Handling