DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

JUL 23 2025

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Remediation of Information Technology-based Material Weaknesses Impacting Financial Auditability

References: (a) Section 1005 of the National Defense Authorization Act for Fiscal Year 2024 (Public Law 118-31)
(b) Secretary of Defense Memorandum, "Secretary of Defense Fiscal Year 2025 Financial Statement Audit Remediation Priorities," December 7, 2024
(c) DoD Chief Information Officer Memorandum, "Accelerated Adoption of Identity, Credential, and Access Management," November 26, 2024
(d) Office of the Secretary of Defense Memorandum, "Secretary of Defense Metric and Governance Reporting for Identity, Credential, and Access Management Deployment and Application On-boarding," March 4, 2025
(e) DoD Instruction 5010.40 "Enterprise Risk Management and Risk Management and Internal Control Program," December 11, 2024

This memorandum outlines strategic approaches to remediate long-standing information technology (IT)-based material weaknesses (MWs) impacting financial auditability. It establishes an initial action plan with deadlines to address multiple IT Notice of Findings and Recommendations (NFRs) related to access control, segregation of duties, interface controls, configuration management, and security management. The Department must successfully remediate these material weaknesses to achieve an unmodified audit opinion as required by reference (a). In support of that objective, all Department of Defense (DoD) Components shall:

- Prioritize and execute the near-term strategies and actions outlined in Attachment 1 to address the IT MWs and improve the DoD's overall auditability.

- Onboard all component Internal Controls Over Reporting - Financial Reporting (ICOR-FR) systems to an approved identity, credential, and access management (ICAM) solution no later than September 30, 2026, as described in references (b), (c), and (d).

- Provide an annual assertion letter using the template provided in Attachment 2, signed by the Component Chief Information Officer (CIO) and Chief Financial Officer (CFO) from DoD Components that have reported IT MWs. This letter, confirming compliance with this directive and detailing implementation progress in addressing those weaknesses, must be submitted to the DoD CIO (DODCIO-IE-ICAM@groups.mail.mil) by September 30 each year until this memorandum is rescinded or cancelled.

These actions are critical activities to comply with existing authoritative guidance, ultimately leading to an unmodified audit opinion, and ensuring the integrity of the Department's

financial systems and statements. Progress against these actions will be governed through the Information Technology Functional Council (ITFC) and the Defense Business Council (DBC).

My point of contact for this matter is Mr. Tyler Harding at samuel.t.harding2.civ@mail.mil or (571) 256-1872.

Katherine Arrington
Performing the Duties of the
Chief Information Officer of the
Department of Defense

Attachments:
As stated

Attachment 1: Near-Term Strategies and Actions

This memo prioritizes and diligently applies the existing guidance issued by the Office of the Under Secretary of Defense (Comptroller) (OUSD(C)) in DoD Instruction 5010.40 "DoD Enterprise Risk Management and Risk Management and Internal Control Program." By focusing on the nine strategies identified in this Appendix, we can collectively address known IT weaknesses and position the Department for a successful FY28 audit.

The DoD CIO will track the nine strategies and associated actions below and report progress quarterly to the ITFC and the DBC. Components should also document and retain evidence that they have completed the following nine strategies to support the Annual Statement of Assurance, signed by the Component's CIO and CFO in addition to providing an annual assertion letter.

Near-Term Remediation Strategies to Achieve an Unmodified Audit Opinion by Priority

Strategy	Action	Action Officers	Deadline	Outcome/Goal
1. Re-evaluate Corrective Action Plans (CAPs) and Plan of Action and Milestones (POA&M) for NFRs contributing to IT Material Weaknesses	Review and update all CAPs in the Advana NFR database (https://advana.data.mil/) and POA&Ms in the Enterprise Mission Assurance Support Service (eMASS) (https://nisp.emass.apps.mil/) to ensure milestones are met within the agreed upon timelines. • CAPs must exist for all IT NFRs contributing to a material weakness • Due dates should not exceed September 30, 2026 • Due dates exceeding September 30, 2026 require Component CIO briefing to DoD CIO justifying dates and planned actions.	System owners	August 30, 2025 (for NFRs received from the 2024 audit)	All CAPs for NFRs contributing to a material weakness are validated to be on track and achievable, ensuring timely remediation of NFR findings and root causes.
2. Identify privileged system and application accounts	Define and document system and application roles, profiles, transactions, resources,	System owners	September 30, 2025	A complete and documented list of privileged users and roles is created and

Strategy	Action	Action Officers	Deadline	Outcome/Goal
	and other activities that are restricted to functional and IT privileged users in accordance with reference (e), DoDI 8520.04, and the DoD ICOR-FR & FS Guide.			maintained, enhancing accountability and security for sensitive operations.
3. Review and update SV-1 diagram illustrating connected/interface systems with documented interface controls.	Review systems owned and update the SV-1 diagram to illustrate all data exchanges and interfaces with external systems.	System owners	September 30, 2025	Complete list of exchanges to and from each system with documented processes designed to ensure complete, accurate, and secure data transmission between systems.
4. Review and update all Information Technology Policies and Standard Operating Procedures (SOP)	Review and update all IT general controls and business process application controls (ITGC/BPAC) policies and SOPs for ICOR-FR systems in accordance with the DoD ICOR-FR & FS Guide (Appendix E), available at https://dod365.sharepoint-mil.us/sites/OSDCOMP-FIAR. Examples include system architecture diagrams, baseline configuration, Risk Management Framework (RMF) accreditation package, risk assessment, security management plan/system security plan, configuration item inventory, access control policies, security event logging criteria, configuration management plans/ patch management procedures, master data change management policies and procedures,	System Owners	September 30, 2025	100% of system owners updated and signed their system-specific ITGC/BPAC policies and SOPs, ensuring they are current and were reviewed within the past 12 months.

Strategy	Action	Action Officers	Deadline	Outcome/Goal
	system design and operation documentation, data strategy/interface plan, and continuity of operation plans.			
5. Develop and implement intra-application segregation of duties (SoD) rules	Document rules defining incompatible functions (i.e., access right assignments) within each individual application.	System owners	September 30, 2025	100% of application owners have written SoD conflicts definitions to enable the prevention and monitoring of incompatible access assignments.
6. Apply and implement the RMF Financial Management (FM) overlay to all ICOR-FR relevant systems.	Assess and authorize all ICOR-FR relevant systems using currently available Rev 4 RMF FM Overlay. Incrementally implement the Rev 5 FM Overlay as each group of National Institute of Standards and Technology (NIST) Control IDs becomes available, apply each increment to subsequent authorization and accreditation processes, and complete the migration to Rev 5. The FM overlays are available at https://cybersecurityks.osd.mil/dodcs/controlsandauthorization/fmoverlay.	System owners	December 31, 2025	100% of financial systems fully implemented and properly applied one of the required FM overlays, demonstrating DoD's commitment to a strong internal control environment over its financial systems.
7. Map application roles to enterprise cross system baseline SoD functional IDs	Map and implement all application roles to corresponding functional IDs in the approved end-to-end cross system baseline SoD rules with the ICAM Service Provider. For systems with technical constraints that cannot complete mapping by March 31,	System owners	Within 1 quarter after application on-boarding to the ICAM service provider, but no later than March 31, 2026	Application roles are mapped to functional IDs, preventing incompatible access provisioning through the component level ICAMs and/or Defense Information Systems Agency (DISA) Federation Hub and accelerating alignment with

Strategy	Action	Action Officers	Deadline	Outcome/Goal
	2026, provide status updates to DoD CIO, and document continuous manual mitigation efforts, with a roadmap for long-term automation.			ICAM requirements.
8. Develop and implement inter-application SoD rules	Document rules defining incompatible access right assignments across applications on the same ICAM Service Provider.	System owners	September 30, 2026	100% of application owners have written definitions of SoD conflicts to enable the prevention and monitoring of incompatible access assignments.
9. Review privileged and non-privileged system and application accounts	Perform and document access reviews for both privileged and non-privileged system and application accounts in accordance with DoDI 8520.04 and the DoD ICOR-FR & FS Guide.	System owners	Ongoing	Accurate and timely system and application account provisioning and deprovisioning through regular and documented access reviews.

Attachment 2: Annual Assertion Letter Template

This template should be adapted by each organization to address the relevant industry and the scope of the audit.

[Component Letterhead]

Date: [Date]

Letter For: Chief Information Officer of the Department of Defense

From: [Component CIO Name], Chief Information Officer, [Component Name]
[Component CFO Name], Chief Financial Officer, [Component Name]

Subject: Annual Assertion of Compliance with IT Remediation Memorandum

This letter provides an assertion of compliance by [Component Name] with the Department of Defense (DoD) direction regarding the remediation of Information Technology (IT)-based material weaknesses impacting financial auditability, as outlined in the memorandum issued by Ms. Katherine Arrington, Performing the Duties of the Chief Information Officer of the Department of Defense on [Date of DoD CIO Memo].

[Component Name] is committed to achieving an unmodified audit opinion by December 31, 2028, as required by Section 1005 of the National Defense Authorization Act for Fiscal Year 2024 (Public Law 118-31). We are actively implementing the strategies and actions outlined in Attachment 1 of the memorandum to address IT material weaknesses and improve the DoD's overall auditability.

Scope:

This assertion covers the implementation and operating effectiveness of IT remediation activities conducted by [Component Name] to address IT-based material weaknesses impacting financial auditability from [Start Date of Reporting Period] to [End Date of Reporting Period]. This scope encompasses progress against the nine strategies outlined in Attachment 1 of the [Date of DoD CIO Memo] memorandum for the following financial systems within [Component Name]: [System A - e.g., the General Ledger System], [System B - e.g., the Procurement System], and [System C - e.g., the Funds Management System]. This assessment includes all related interfaces and supporting infrastructure associated with these systems, without requiring a specific, itemized listing of each interface. [System X - e.g., the Legacy Reporting System], scheduled for decommissioning on [Date - e.g., December 31, 2024], is excluded as it is not considered material to financial reporting.

Basis for Assertion:

This assertion is based on ongoing monitoring activities, including the tracking of key performance indicators (KPIs) related to each of the nine strategies; periodic internal reviews conducted by [Component Name]'s internal audit function (or equivalent) to assess the design and effectiveness of remediation efforts; validation of implemented remediation actions through

control testing and documentation review to ensure effective mitigation of material weaknesses; regular progress reporting to [Component Name]'s leadership and the DoD CIO; and, if applicable, the results of independent verification and validation (IV&V) activities performed by a third party.

Assertion of Compliance:

Based on the scope and basis described above, I assert that [Component Name] is compliant with the CIO memorandum and is making satisfactory progress towards the remediation of IT-based material weaknesses as of [Date of Assertion - same as Date at top of memo].

Implementation Progress:

The following provides a summary of [Component Name]'s progress in implementing the strategies and actions outlined in Attachment 1:

- **Strategy 1: Re-evaluate CAPs and POA&Ms:** [Provide a concise summary of progress, including the number of CAPs/POA&Ms reviewed, updated, and validated. Include any challenges or deviations from planned timelines.]
- **Strategy 2: Identify Privileged System and Application Accounts:** [Provide a concise summary of progress, including the percentage of systems for which privileged accounts have been identified and documented.]
- **Strategy 3: Provide SV-1 Diagram with Interface Controls:** [Provide a concise summary of progress, including the percentage of systems for which SV-1 diagrams and interface controls have been documented.]
- **Strategy 4: Review and Update IT Policies and SOPs:** [Provide a concise summary of progress, including the percentage of ITGC/BPAC policies and SOPs reviewed and updated.]
- **Strategy 5: Develop and Implement Intra-Application SoD Rules:** [Provide a concise summary of progress, including the percentage of applications for which SoD rules have been defined and documented.]
- **Strategy 6: Apply and Implement RMF FM Overlay:** [Provide a concise summary of progress, including the percentage of financial systems that have fully implemented the required FM overlays, and the progress toward migrating to Rev 5.]
- **Strategy 7: Map Application Roles to Enterprise Cross System Baseline SoD Functional IDs:** [Provide a concise summary of progress, including the number of application roles mapped to functional IDs and the status of systems with technical constraints requiring manual mitigation.]
- **Strategy 8: Develop and Implement Inter-Application SoD Rules:** [Provide a concise summary of progress, including the percentage of applications for which inter-application SoD rules have been defined and documented.]

- **Strategy 9: Review Privileged and Non-Privileged Accounts:** [Provide a concise summary of progress, including the frequency and scope of access reviews.]

ICAM Onboarding:

[Provide a statement of progress towards onboarding ICOR-FR systems to an approved ICAM solution. Include the number of systems onboarded to date and the projected completion date for all remaining systems. If the September 30, 2026, deadline will not be met, provide a detailed explanation and mitigation plan.]

Challenges and Mitigation Strategies:

[Identify any significant challenges encountered during implementation and the strategies being employed to mitigate those challenges. This section is crucial for transparency and proactive problem-solving.]

Conclusion:

[Component Name] is committed to achieving full compliance with the IT remediation directive and ensuring the integrity of the Department's financial systems and statements. We will continue to monitor our progress, address any challenges that arise, and provide updates to the DoD CIO as needed.

[Component CIO Signature]	**[Component CFO Signature]**
[Component CIO Name]	**[Component CFO Name]**
Chief Information Officer, [Component Name]	**Chief Financial Officer, [Component Name]**
[Contact Information (Phone Number, Email Address)]	**[Contact Information (Phone Number, Email Address)]**

This example provides a starting point for creating your own Annual Assertion Letter. Remember to tailor it to your specific circumstances and consult with relevant experts.