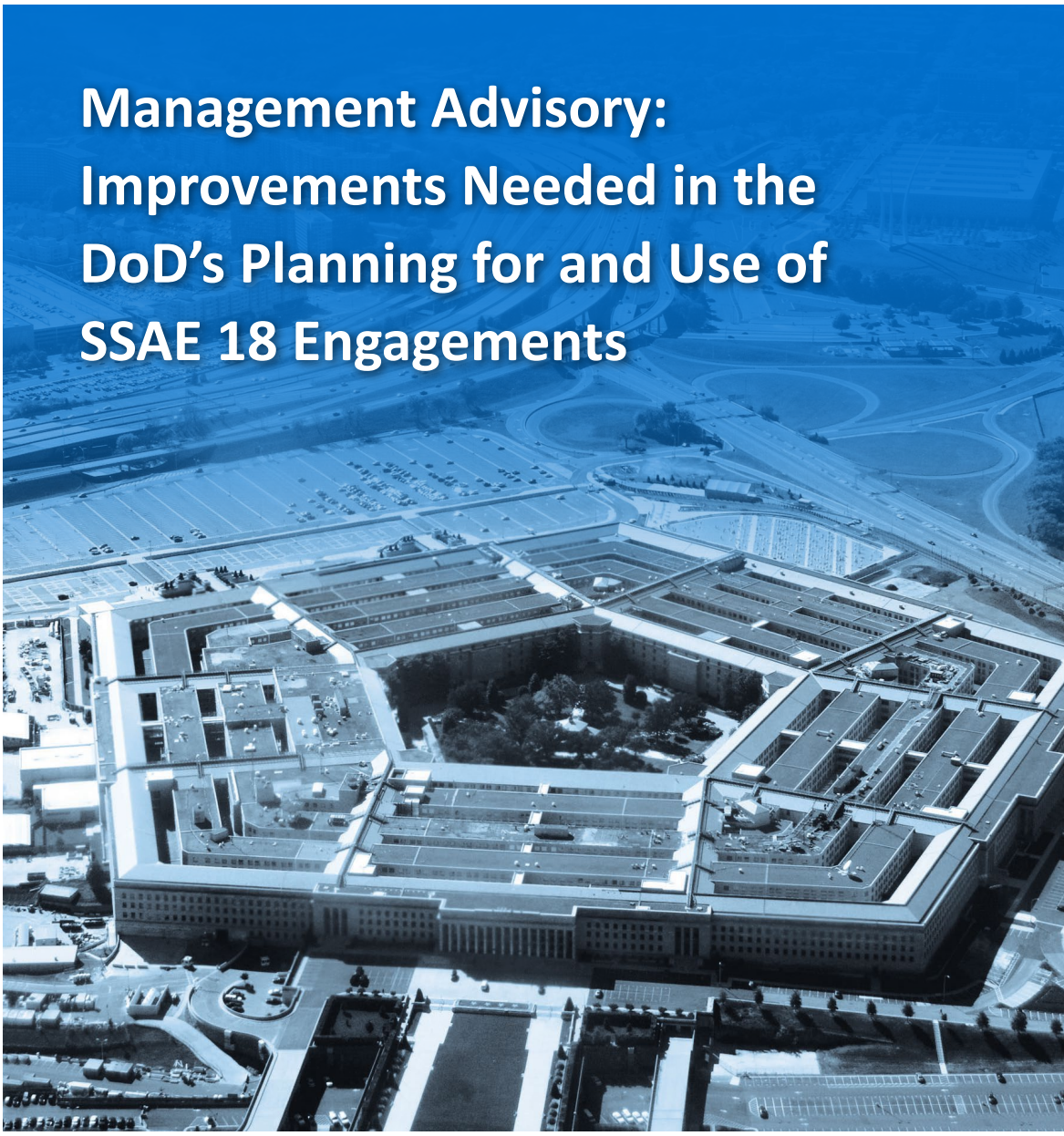
Report No. DODIG-2025-044

INSPECTOR GENERAL

U.S. Department of Defense

NOVEMBER 22, 2024

Management Advisory: Improvements Needed in the DoD's Planning for and Use of SSAE 18 Engagements



INDEPENDENCE ★ INTEGRITY ★ EXCELLENCE ★ TRANSPARENCY


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

OFFICE OF INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

November 22, 2024

MEMORANDUM FOR THE UNDER SECRETARY OF DEFENSE (COMPTROLLER)/
CHIEF FINANCIAL OFFICER, DOD

SUBJECT: (U) Management Advisory: Improvements Needed in DoD's Planning for and Use of SSAE 18 Engagements (Report No. DODIG-2025-044)

This final report provides the results of the DoD Office of Inspector General's review of whether the DoD is effectively planning for and using American Institute of Certified Public Accountants' Statement on Standards for Attestation Engagements No. 18 engagements, as amended, to improve financial statement audit readiness and efficiency. We previously provided copies of the draft report and requested written comments on the recommendations. We considered management's comments on the draft report when preparing the final report.

This report contains recommendations that are considered unresolved because the Office of the Under Secretary of Defense (Comptroller), Chief Financial Officer, DoD, did not fully address the recommendations presented in the report. Therefore, the recommendations remain open. We will track these recommendations until management has agreed to take actions that we determine to be sufficient to meet the intent of the recommendations and management officials submit adequate documentation showing that all agreed-upon actions are completed.

DoD Instruction 7650.03 requires that recommendations be resolved promptly. Therefore, please provide us within 30 days your response concerning specific actions in process or alternative corrective actions proposed on the recommendations. Send your response to audfmr@dodig.mil.

If you have any questions, please contact me at

FOR THE INSPECTOR GENERAL:

Lorin T. Venable

Lorin T. Venable, CPA
Assistant Inspector General for Audit
Financial Management and Reporting


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Executive Summary

The objective of this review was to determine whether the DoD effectively planned for and used Statement on Standards for Attestation Engagements No. 18 (SSAE 18), as amended, to improve its financial statement audit readiness and efficiency. We assessed DoD management's planning for and use of System and Organization Controls 1 (SOC 1) reports on internal controls performed by service organizations. We also assessed DoD implementation of complementary user entity controls (CUECs) by organizations that relied on the service organizations and the internal controls described in the service organizations' SOC 1 reports.

This management advisory addresses a deficiency by which DoD service organizations did not always develop their reporting documentation to include all relevant internal controls to all appropriate user entities. Furthermore, the user entities were not always engaged, communicative, and proactive, and they did not always prioritize the design and implementation of CUECS.

Although the DoD spent more than $15.5 million in FY 2023 across 30 SSAE 18 engagements, the auditors who audit DoD entities' financial statements did not always rely on the service organizations' SOC 1 reports and internal controls described within the reports. If the auditors are unable to rely on the SOC 1 reports and internal controls identified within the reports, efficiencies are lost because the auditor will perform additional testing, increasing the cost of the financial statement audits and the audit burden on the service organizations and user entities.

We are providing this advisory, rather than a full report, so that officials from the Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, DoD can promptly evaluate and verify potential internal control weaknesses and initiate corrective actions.

Introduction

Objective

The objective of this management advisory was to determine whether the DoD effectively planned for and used Statement on Standards for Attestation Engagements No. 18 (SSAE 18), as amended, to improve its financial statement audit readiness and efficiency.[1] We assessed DoD management's planning for and use of System and Organization Controls 1 (SOC 1) reports on internal controls performed by service organizations.[2] We also assessed DoD implementation of complementary user entity controls (CUECs) by organizations that relied on the service organizations and the internal controls described in the service organizations' SOC 1 reports.

We prepared this management advisory in accordance with the Council of the Inspectors General for Integrity and Efficiency's Quality Standards for Federal Offices of Inspector General, which require that we conduct our work with integrity, objectivity, and independence.

Background

The DoD's Use of Service Organizations

The "Chief Financial Officers Act of 1990" requires the DoD to prepare audited financial statements.[3] To comply with this requirement, the DoD produces a set of financial statements that consolidates the financial activity of more than 60 DoD reporting entities, including the Military Departments, Defense agencies, and DoD field activities. The consolidation of these DoD entities makes up the DoD Agency-Wide financial statements. This consolidation process requires that each DoD entity develop, document, implement, and monitor a set of internal controls over financial reporting. [4] The DoD's current goal is to achieve an unmodified opinion on the DoD and DoD entities' financial statements by FY 2028; as legislated by Congress within the National Defense Authorization Act for FY 2024.[5]

---

1 American Institute of Certified Public Accountants, "Statement on Standards for Attestation Engagements," No. 18, April 2016.

2 Service organizations are also referred to as service providers throughout the DoD and commercial sector.

3 Public Law 101-576, "Chief Financial Officers Act of 1990," November 15, 1990.

4 AICPA's Clarified Statements on Auditing Standards (AU-C) section 940 defines internal control over financial reporting as a process effected by those charged with governance, management, and other personnel, designed to provide reasonable assurance regarding the preparation of reliable financial statements in accordance with the applicable financial reporting framework.

Office of Management and Budget (OMB) Circular No. A-123, "Management's Responsibility for Enterprise Risk Management and Internal Control," July 15, 2016, defines internal control as an integral component of an organization's management that provides reasonable assurance that the following objectives are achieved: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. Internal controls is a broad term and will be used throughout the report.

5 Public Law 118-31, "National Defense Authorization Act for Fiscal Year 2024," December 22, 2023 requires the Secretary of Defense to ensure that the DoD receives an unmodified opinion on the financial statements of the Department by not later than December 31, 2028.

Many of these DoD entities are interdependent and rely on each other to provide specialized services, such as logistics, contract administration, information technology, accounting and payment support, and the necessary internal controls for these services. Many of these interdependent entities that provide internal controls over functions that result in financial transactions are considered service organizations, and the customers of the services are the user entities.

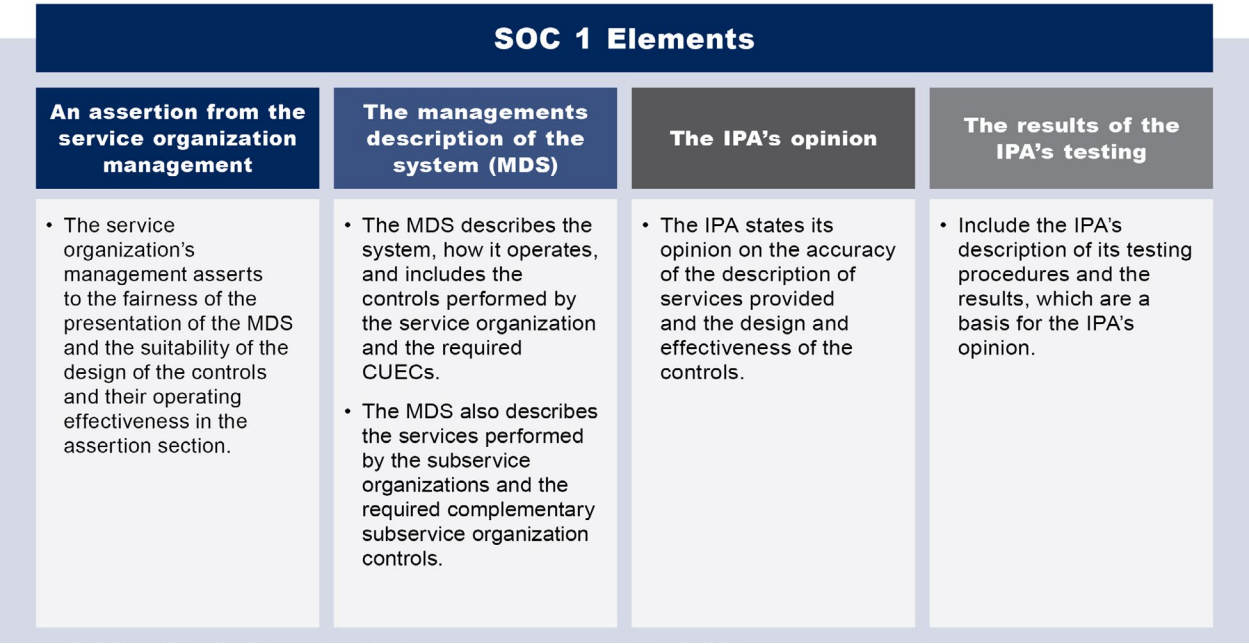
The DoD identified more than 50 shared processes as significant to financial statements, including more than 30 internal to DoD and more than 20 other processes performed by other Federal agencies and commercial service organizations. These processes improve DoD efficiency and standardize tasks related to DoD operations, financial management, and financial reporting.

DoD entities gain efficiencies when several entities can have services performed by one service organization instead of attempting to perform the service and internal controls themselves. A SSAE 18 examination that results in a SOC 1 report allows the service organization internal controls to be tested once and relied upon by all the user entities' auditors instead of being tested multiple times for multiple user entities for a given time period. A SOC 1 report includes an assertion from the service organization management, management's description of the system (MDS), Independent Public Accounting firm's (IPA's) opinion, and results of the IPA's testing.[6] Figure 1 demonstrates the SOC 1 elements included in the report.[7]

[6] AICPA SSAE No. 18 defines assertion as any declaration or set of declarations about whether the subject matter is in accordance with (or based on) the criteria.

[7] An optional section may be included in the SOC 1 report for other information that management feels provides additional insight into the service. The other information section is not audited.

Figure 1. System and Organizational Controls 1 (SOC 1) Elements



Note: The MDS identifies the services covered, associated time period for the description (or in the case of a type 1 report, the associated date for the description), control objectives specified by management or an outside party, party specifying the control objectives (if not specified by management), and related controls. The service organization's system are the policies and procedures designed, implemented, and documented by management of the service organization to provide user entities with the services covered by the service auditor's report.

Source: The DoD OIG.

In the MDS, the service organization documents controls performed for all user entities. To prevent overlap, the service organization and user entities should enter into a written agreement such as a memorandum of understanding in which the service organization and user entity agree to the services provided, any costs associated with the service, and a frequency at which a user entity may monitor the service organization's performance.

During a financial statement audit, the user entity's auditor should be able to understand the agreement, test and rely upon the controls, and have confidence that the internal controls are effective and provide reasonable assurance that the internal control would not allow a material misstatement on the financial statements. Figure 2 describes the roles of the three parties involved in a user entity and service organization relationship. If there is a failure in the design, implementation, or operation of internal controls performed by any of the three parties, then the user entity and its auditor may no longer rely on the service organization internal controls described in the SOC 1 report.[8]

[8] The user auditor may be either the DoD OIG or IPA.

Figure 2. User Entity and Service Organization Roles

Source: The DoD OIG.

Service Organizations and Internal Controls

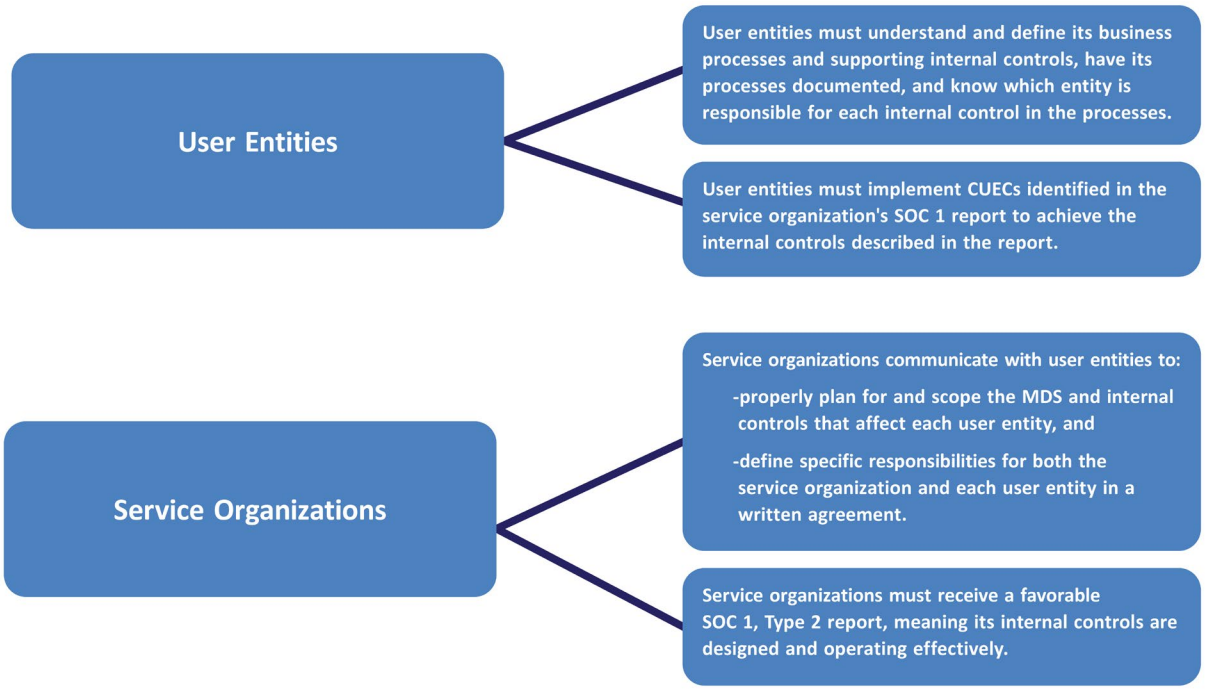
The DoD and its entities are required to identify and document internal controls over financial reporting. OMB Circular No. A-123 defines management's responsibility for internal controls. Part of the process to identify and document internal controls over financial reporting is to identify and monitor service organizations that perform internal controls on their behalf. Once identified, these service organizations must develop, implement, and document effective, reliable internal controls for all relevant user entities.

Each service organization may provide services and internal controls to one or several user entities. As a result, user entity auditors, referred to as user auditors, may need to test the internal controls provided by the service organization. This testing would aid the user auditor to rely on the internal controls to be designed, implemented, and operating effectively, and provide reasonable assurance that balances on the financial statements are accurate. The user entities and their financial statement auditor determine whether the internal controls provided by the service organization are significant to the user entities' financial statements.

To increase efficiency, the service organizations should develop a MDS that describes the internal controls in place. The service organization engages with an IPA to evaluate and test the service organization internal controls and provide an opinion on the description, design, and operating effectiveness of the internal controls. The result is a SOC 1 report that the service organization provides to the user entities, which then provide the report to their user auditor.

According to AT-C Section 320, "Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Controls Over Financial Reporting," for a user auditor to rely on a SOC 1 report and the internal controls described within a SOC 1 report, the user entities and service organizations have the responsibilities shown in Figure 3.

Figure 3. User Entities' and Service Organizations' Responsibilities



Source: The DoD OIG.

SSAE 18 engagements can help user auditors rely on the adequacy of the process and internal controls described within the SOC 1 report without having to perform their own audit procedures over the service organizations internal controls. Without an SSAE 18 engagement, auditors of each user entity would likely need to separately test the service organization's internal controls, resulting in duplicative testing of the same internal controls.

Figure 4 identifies the three types of auditors involved in an SSAE 18 engagement and describes the role of each.

Figure 4. Types of Auditors Involved in an SSAE 18 Engagement

Source: The DoD OIG.

In addition, the user entities need to incorporate complementary user entity controls or CUECs to ensure that all the control objectives identified within the SOC 1 report are fully implemented.[9] These CUECs are outlined by the service organization in the SOC 1 report and intended to provide direction for the user entity on how to design and implement internal controls for the user entity to ensure that the user entity CUECs are effectively functioning to complement the service organization internal controls. All relevant controls, including the service organization's internal controls and the user entity CUECs, must all function effectively for the internal controls over financial reporting in the SOC 1 report to be relied on by the user auditor.

One example of a user entity and service organization relationship is the Marine Corps use of the Defense Agencies Initiative (DAI) application from the Defense Logistics Agency (DLA). The DLA provides an accounting application, DAI, as a service for 27 user entities, including the Marine Corps. Instead of auditors for each of these 27 user entities repeating tests of the same DAI system internal controls within the application, the DoD has elected to have DAI examined through an SSAE 18 engagement.

The DAI Program Management Office provides internal control activities related to eight control objectives so user entities can rely on DAI for financial management and reporting. To ensure the reliability of DAI, user entities must also design and implement additional internal controls associated with the DAI system. These additional internal controls are called CUECs. DAI management also relies on its subservice organizations, including the DLA's Defense Automated Addressing System program, which provides data transmissions services for the DAI system. The Defense Automated Addressing System program is a subservice organization that performs complementary subservice organization controls necessary to meet DAI's control objectives.[10]

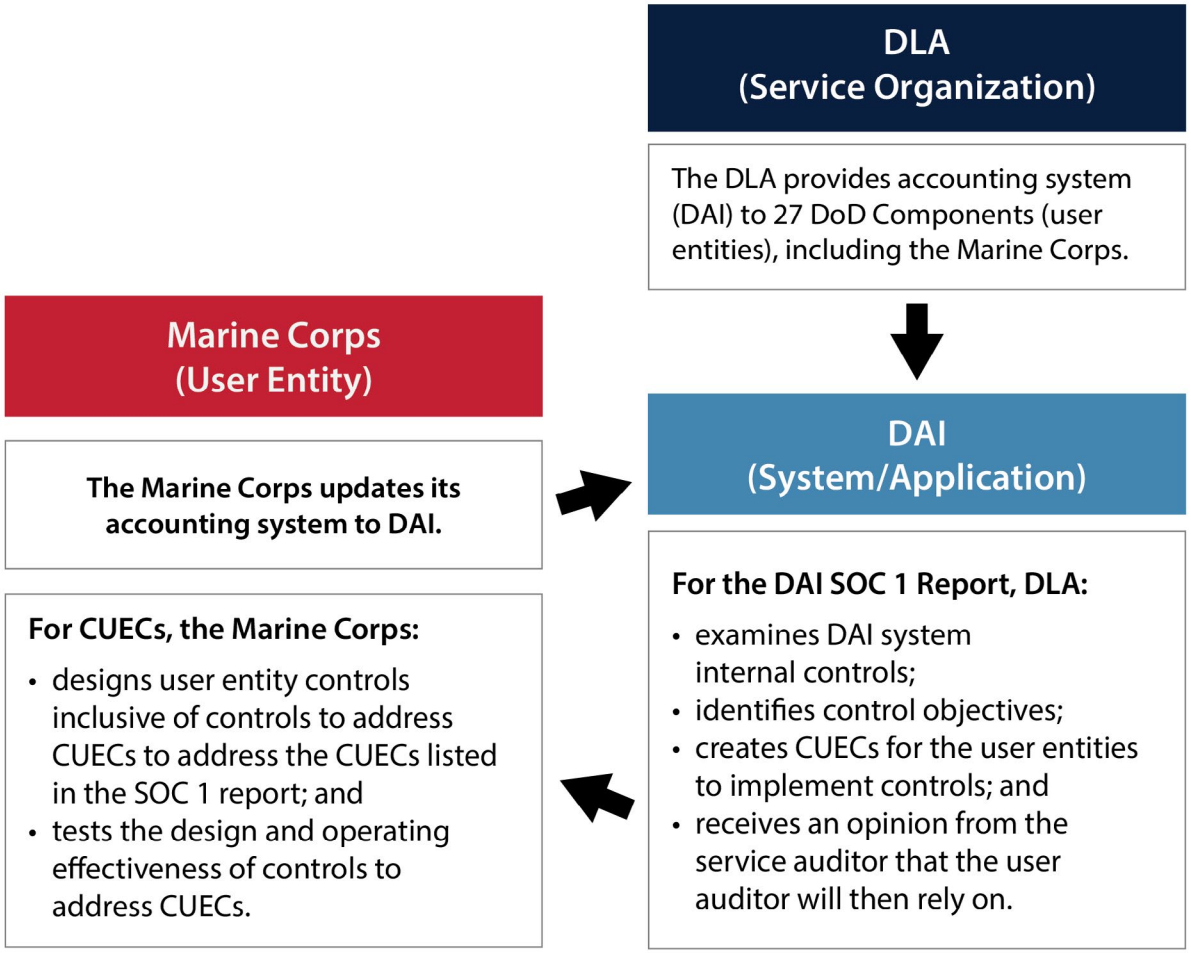
DAI users are required to implement many CUECs. For example, access controls are required to provide reasonable assurance that access to DAI data is restricted to authorized users. In this example, the Marine Corps and DAI Program Management Office must effectively perform internal controls, for which they are responsible, for the Marine Corps and its user auditor to rely on DAI's access controls. Figure 5 illustrates the user entity and service organization relationship between the Marine Corps' use of DAI from the DLA.

[9] AICPA AT-C Section 320 defines control objectives as the aim of specified controls at the service organization. Control objectives address the risks that controls are intended to mitigate.

AICPA AT-C Section 320 defines CUECs as controls that, in the design of the service organization's system, management of the service organization assumes will be implemented by user entities and are necessary to achieve the control objectives stated in management's description of the service organization's system.

[10] AICPA AT-C Section 320 defines complementary subservice organization controls as controls that, in the design of the service organization's system, management of the service organization assumes will be implemented by the subservice organizations and are necessary to achieve the control objectives stated in management's description of the service organization's system.

Figure 5. Marine Corps Use of the Defense Agencies Initiative from the Defense Logistic Agency



Source: The DoD OIG.

SOC 1 Reporting in the DoD

The Office of the Under Secretary of Defense (Comptroller) (OUSD[C]) identified 30 systems and processes performed by internal DoD service organizations that were material to the FY 2023 financial statement audits. The DoD contracts with five IPAs to perform SSAE 18 engagements for these 30 systems and processes. In FY 2023, the DoD spent more than $15.5 million for 30 SSAE 18 engagements performed by the IPAs.

There are two types of SOC 1 reports. SOC 1, Type 1 reports are an examination of the service organization's description, or design, of its internal controls as of a certain date.[11] In a Type 1 report, the IPA provides an opinion on a service organization's MDS, and the

[11] Type 1 reports are useful for service organization management to determine the status of the design of internal controls within their system and documented within their MDS. Internal controls within type 1 reports cannot be relied on by user auditors when auditing financial statements due to the opinion not ensuring that these internal controls were operating effectively throughout the audit engagement.

design of the internal controls as of a certain date. Type 2 reports are an examination of the suitability of the design and operating effectiveness of those internal controls over a time period, which has traditionally been October 1 through June 30 for the DoD. In a Type 2 report, the IPA provides an opinion on a service organization's MDS, the design of the internal controls, and the operating effectiveness of the internal controls throughout the period under examination.

The reports are finalized by August 15, allowing the user auditor to consider the results for the financial statement audit for the current fiscal year ending September 30.[12] Once a user auditor determines the internal controls within the SOC 1 report may be relied on, the user auditor may request that the service organization provide a bridge letter confirming the internal controls identified within the SOC 1 report remained in place for the remainder of the fiscal year. For the DoD, the bridge letter would cover July 1 through September 30.

Service auditors may issue unmodified, qualified, disclaimer, or adverse opinions within a SOC 1 report depending on the accuracy of the MDS, the design of the system internal controls, and the operating effectiveness of the system internal controls. Figure 6 demonstrates the types of opinions that auditors can issue.

[12] OUSD Memorandum, "Improving Reporting on Service Provider Controls," February 26, 2016 required SOC 1 reports be issued by August 15 of each fiscal year. The August 15 date may not be achievable because of acquisition lead times or work efforts of the service organization or service auditor.

Figure 6. Types of Auditor's Opinions

Source: The DoD OIG.

For SOC 1 reports that receive unmodified opinions, user entities and user auditors can rely on the service organizations' internal controls. In this way, SSAE 18 engagements can add efficiency to the financial statement auditing process by allowing internal controls to be tested once rather than multiple times. In our example of the Marine Corps use of DAI, DAI had received an unmodified opinion. The Marine Corps and the other 26 user entities may rely on DAI's internal controls as part of their control environment assuming they implemented the required CUECs. Additionally, because effective internal controls provide reasonable assurance that financial information is accurate, user auditors can potentially reduce the number of sample items selected to test balances on the financial statements.

The DAI SOC 1 report is one of 15 DoD SOC 1 reports that achieved unmodified opinions in FY 2023. An additional 14 DoD SOC 1 reports received qualified opinions, and one DoD service organization received an adverse opinion on its SOC 1 report. When issuing the qualified opinions, the IPAs document in their reports a description of the deficiencies and affected internal controls and issue Notices of Findings and Recommendations (NFRs) to the service organizations.[13] Figure 7 lists the DoD service organizations undergoing SSAE engagements and the processes or systems involved in the engagements, resulting in 15 unmodified opinions, 14 qualified opinions, and 1 adverse opinion.

[13] An NFR is the mechanism of communicating to management findings identified throughout DoD financial statement audits and SSAE 18 engagements.

Figure 7. FY 2023 SSAE 18 Opinions

Unmodified	Qualified	Adverse
Chief Digital and Artificial Intelligence Office (CDAO) Advancing Analytics (ADVANA)		
Defense Finance and Accounting Service (DFAS) Civilian Pay	**Army** General Fund Enterprise Business System (GFEBS)	
DFAS Contract Pay	**Army** Munitions Mgmt	
DFAS Vendor Pay-Defense Enterprise Accounting and Management System (DEAMS)	**Department of the Air Force (DAF)** DEAMS	
DFAS Vendor Pay-Navy Enterprise Resource Planning System (ERP)	**Defense Contract Management Agency (DCMA)** Contract Pay	
DFAS Disbursing Service	**DCMA** Government Contract Property Administration System (GCPAS)	
DFAS Enterprise Local Area Network (ELAN)	**DFAS** Financial Reporting	
Defense Manpower Data Center (DMDC) Defense Civilian Personnel Data System (DCPDS)	**DFAS** Defense Cash Accountability System (DCAS)	
DMDC Defense Travel System (DTS)	**DFAS** Military Pay	
Defense Logistics Agency (DLA) Defense Agencies Initiative (DAI)	**DFAS Vendor Pay - Computerized Accounts** Payable System - Windows (CAPS-W)	
DLA Government Furnished Property (GFP)	**DFAS** Vendor Pay -GFEBS	
DLA Wide Area Workflow (WAWF)	**DFAS** Vendor Pay -Integrated Accounts Payable System (IAPS)	
Defense Information Systems Agency (DISA) Automated Time and Attendance System (ATAAPS)	**DFAS** Vendor Pay -One Pay	
DISA Hosting Services	**DLA** Defense Automated Addressing System (DAAS)	
DISA Stratus Infrastructure as a Service (IaaS)	**DLA** Defense Property Accountability System (DPAS)	**DFAS** Vendor Pay-DAI
15	14	1

Source: The DoD OIG.

Timeline of the Service Provider Working Group

In FY 2005, the OUSD(C) established the Financial Improvement and Audit Remediation (FIAR) Directorate to standardize and document the DoD's efforts to develop more effective financial management processes.[14] The FIAR Directorate's key focus areas were internal controls, financial information accuracy, and systems improvement. To improve internal controls, the FIAR Directorate established the Service Provider Working Group (SPWG) in FY 2016 to provide awareness and solutions for issues related to processes and policies that may impede the DoD's auditability. The SPWG is chaired by the FIAR Directorate and includes representatives from user entities, service organizations, and auditors.

Service Organizations Are a Material Weakness

The DoD OIG began reporting service organizations as a DoD Agency-Wide material weakness in FY 2021 and continued to do so through FY 2023. For example, the DoD OIG determined that the DoD did not:

- adequately monitor the use of service organizations or the design and implementation of complementary user entity controls (CUECs) to ensure compliance with the Green Book;[15]
- fully document, implement, test, or monitor their CUECs; or
- provide corrective action plans to remediate service organization notices of findings and recommendations or consider the impact of service organizations within the DoD's existing internal control environment.

Further, the DoD service organizations received qualified or adverse opinions because their internal controls were not suitably designed or did not operate effectively to achieve the control objectives of the service organization. For example, multiple SOC 1 reports were issued with qualified opinions because the service organizations did not design and implement effective internal controls to meet control objectives. Additionally, service organizations did not ensure access to the systems were restricted to authorized users, which increased the risk to data and other internal controls.

The DoD OIG also determined that the user entities did not have procedures to oversee and monitor the service organizations and did not design or implement CUECs. The deficiencies of the service organizations and user entities decreased the reliability and benefit of the SSAE 18 engagements and increased risk that balances in the DoD Agency-Wide financial statements may be materially misstated. The Secretary of Defense listed CUECs as one of the DoD's financial statements audit priorities in FY 2023.

[14] "Financial Improvement and Audit Readiness" refers to FY 2005 through FY 2017, and "Financial Improvement and Audit Remediation" refers to FY 2018 to FY 2024.

[15] The Government Accountability Office's Standard for Internal Control in the Federal Government, GAO-14-704G, current version dated September 10, 2014, is commonly referred to as the GAO Green Book.

Improvements Are Needed in the DoD's Planning for and Use of SSAE 18 Engagements

The DoD made progress planning for and using SSAE 18 engagements and received unmodified opinions on 15 of 30 FY 2023 SSAE 18 engagements.[16] However, more work is needed to improve the effectiveness and efficiency of the DoD's SSAE 18 engagements. Specifically,

- DoD service organizations did not always develop MDSs that included all relevant internal controls to all appropriate user entities or contained all relevant user entities that relied on a service organization's internal controls; and
- user entities were not always engaged, communicative, or proactive in working with the service organizations, and user entities did not always prioritize the design and implementation of CUECs because of a lack of monitoring by OUSD(C) and the service organizations.

The DoD gained insights from receiving a combined 173 NFRs on the deficiencies that the IPA and DoD OIG identified through their financial statement audits and SSAE 18 engagements and is in the process of completing corrective actions on those NFRs. The NFRs identified that some user entity auditors did not or could not rely on the SOC 1 reports and the internal controls described within the reports, which negated some benefits of the DoD conducting SSAE 18 engagements.

Furthermore, if a service organization receives a qualified, disclaimer, or adverse opinion on its SOC 1 report; the internal controls described in the SOC 1 report are not properly designed; or if the user entity did not design and implement CUECs, then user auditors cannot rely on service organizations' internal controls or CUECs. This has resulted in less reliance on internal controls and caused more substantive-based audit approaches that required large samples and more resources from all parties to execute the collective financial statement audits.

User Entities Should Document Processes and Internal Controls and Coordinate with Service Organizations

User entities and user auditors were not always able to rely on SOC 1 reports and the internal controls described within them. Even though the OUSD(C) established the SPWG to address communication issues, this process remained ineffective in completely remediating weaknesses in the SOC 1 process. Specifically, the SOC 1 reports did not always report on all relevant internal controls to all relevant user entities or contain all relevant user entities that rely on a service organization's internal controls. This inconsistency occurred

[16] For FY 2022, DoD service organizations produced 28 SOC 1 reports where there were 14 unmodified opinions, 11 qualified opinions, 2 adverse opinions, and 1 disclaimer of opinion.

because communication and coordination roadblocks still exist between some service organizations and their user entities, and not all user entities documented their processes and internal controls.

For example, the Defense Contract Management Agency (DCMA), a service organization, and the Department of the Air Force (DAF) did not effectively communicate with each other.[17] For the FY 2023 DAF financial statement audits, the DAF and its user auditor requested information and meetings from DCMA in addition to its SOC 1 report to address audit requests from the DAF user auditor. Instead of meeting, DCMA officials asked the DAF and its user auditors submit written information requests. While DCMA offered limited written responses, this process did not provide the DAF with enough information to satisfy the audit requests from the DAF user auditor.[18]

In another example, the Defense Health Program (DHP), U.S. Special Operations Command (USSOCOM), and other reporting entities used the Department of the Army's General Fund Enterprise Business System (GFEBS) for financial management and reporting. The Army produced a MDS on GFEBS internal controls specific to the DHP. The Army did not identify USSOCOM as a user entity of GFEBS or include USSOCOM in the MDS for the GFEBS SOC 1 report.

The GFEBS Program Management Office acknowledged that USSOCOM has a 2016 agreement with the Army to "grant the USSOCOM auditors and Inspector General (IG) staff access to all documentation, personnel, and information." However, the GFEBS Program Management Office and Army stated that they were uncertain whether the 2016 agreement was sufficient or enforceable or whether the funding existed to include the USSOCOM needs within the report. This communication breakdown did not allow the USSOCOM user auditor to obtain sufficient information on the internal controls relevant to the USSOCOM financial statements in FY 2022 and required additional testing in FY 2023.

Documenting an end-to-end process for a successful SOC 1 report is not solely the responsibility of the service organizations. User entities play a significant role in documenting processes, coordinating with service organizations, and monitoring CUECs for their financial statements. The OMB has determined that user entities remain responsible for establishing CUECs for the service organization's internal controls and retain the overall responsibility and accountability for all internal controls related to the processes provided by the service organization. The user entities must also monitor the process to ensure that the CUECs are effective.[19] For example, USSOCOM did not develop process narratives that clearly identified and communicated with all service organizations, including the Army, and all information systems relevant to USSOCOM's

[17] DCMA service auditors issued qualified opinions for both the FY 2022 and FY 2023 SOC 1, Type 2 reports, based on separate issues related to access controls.

[18] OUSD Memorandum, "Supporting Auditor Requests During Financial Statement Audits and Examinations," August 29, 2017.

[19] OMB Circular No. A-123.

financial statements, including GFEBS. Once USSOCOM addresses this deficiency, it would be better positioned to coordinate with the Army and its other service organizations to identify applicable internal controls, identify user entity responsibilities, develop agreements with service organizations, and advocate for additional service organization internal controls deemed necessary to be examined as a part of the SSAE 18 engagement in support of the USSOCOM financial statements.

Although the FIAR SPWG has promoted communication among the SSAE 18 engagement community by providing a forum for the service organizations, user entities, and auditors, the service organizations and user entities continued to have communication problems. The user entities did not always identify and monitor internal controls provided by service organizations. The user entities were not effectively documenting internal controls over the processing and reporting of financial transactions; identifying what internal controls organizations are responsible for; or having meaningful communication with service organizations. The service organizations and user entities received recommendations through NFRs for documenting and monitoring processes and internal controls and thus, we are not making recommendations to the service organizations and user entities. The Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, DoD, should develop and implement policies and procedures to coordinate with, monitor, and hold user entities accountable for identifying their service organizations, and develop and implement procedures to strengthen communication between the user entities and service organizations, including development of service-level or equivalent agreements that detail roles and responsibilities for each party.

User Entities and Service Organizations Should Design and Implement CUECs to Realize the Benefits of SOC 1 Reports

DoD entities did not establish policies and procedures to address the design and implementation of CUECs to allow user auditors to rely on SOC 1 reports and the internal controls described within them. In FY 2022, the IPAs and DoD OIG auditors issued 79 NFRs related to the design and implementation of CUECs.[20] The application of CUECs by user entities is necessary to achieve the related control objectives stated in the SOC 1 reports. Without proper design, implementation, and monitoring of CUECs, the user entity cannot provide evidence that the information it provided to the service organization is complete, accurate, timely, and authorized. User auditors determine whether user entities have established internal controls to provide reasonable assurance over their use of the service organization.

[20] During the FY 2023 DoD financial statement audit, 68 percent of the NFRs identified in this report were reissued and 32 percent were closed; therefore, the conditions identified in FY 2022 remain applicable.

During the FY 2022 and 2023 DoD financial statement audits, we found that user entities did not always design effective CUECs. For example, the Department of the Navy (DON) received NFRs due to not designing CUECs for Defense Finance and Accounting Service (DFAS) SOC 1 reports. This resulted in the DON user auditors not being able to rely on DFAS' internal controls over Fund Balance with Treasury accounting functions that are material to the DON financial statements. DON management had not established a remediation plan completion date for designing CUECs for DFAS SOC 1 reports.[21] In another example, we identified that USSOCOM did not complete a comprehensive CUEC evaluation applicable to its organization, and the U.S. Transportation Command (USTRANSCOM) did not complete a formal analysis to identify CUECs for which it is responsible. Without completing these initial reviews, USSOCOM and USTRANSCOM were not able to determine which CUECs were applicable to their control environment to ensure all relevant internal controls were fully designed.

User entities did not always effectively implement CUECs as designed. We identified 32 NFRs regarding the lack of properly implemented CUECs. Although these user entities were aware and had local policies and procedures in place for implementing CUECs, the user entities did not always demonstrate that they implemented and effectively operated CUECs. For example, the Missile Defense Agency did not implement a CUEC identified in the Advancing Analytics system SOC 1 report designed to ensure common access cards were revoked within required timeframes upon employee separation or termination. As a result, the Missile Defense Agency did not have internal controls in place to ensure access was only granted to authorized individuals, which could lead to the compromise of information system data.

We also identified instances in which the DON did not implement CUECs established by DFAS. For example, the DON was unable to provide 8 of 10 access request forms to demonstrate that any DON users with access to DFAS systems and data always maintained an appropriate DoD clearance and background checks. Failure to implement the CUEC increased the risk that the security practices are improperly implemented and internal controls are inconsistently applied, and it may lead to inappropriate access to DFAS systems and data.

In another example, although the DHP issued a CUEC policy, the DHP IPA found that the DHP did not fully implement the policy to ensure CUEC compliance. Further, the DHP did not implement a formalized process to map and document existing internal control activities to required CUECs, or it did not assess where internal control gaps may exist based on required CUECs. DHP management stated that its current remediation plan to close all NFRs related to implementation of CUECs is scheduled for September 30, 2025.

[21] DFAS Disbursing Service SOC 1 report and DFAS Financial Reporting SOC 1 report.

The DoD Needs to Improve SOC 1 Report Reliability

User entities did not have proper policies or procedures for designing, implementing, monitoring, communicating, and coordinating the impact of service organization internal controls identified in the SOC 1 reports to the user entities' processes. Furthermore, user entities did not implement CUECs in a timely manner. DoD officials stated they were not able to implement CUECs due to the large amount of CUECs across the DoD's systems. User entities continued to prioritize addressing financial statement NFRs over completing corrective actions on NFRs associated with designing and implementing CUECs, and monitoring service organizations. Without prioritizing the latter, the DoD may not make progress in meeting the congressional mandate of an unmodified opinion by 2028.

We reviewed responses to the FY 2023 Agency-Wide information technology (IT) questionnaire and interviewed user auditors to determine whether they relied on the internal controls within the SOC 1 reports. We also reviewed the responses to understand the user auditors' assessment of the user entities' progress in designing, implementing, and monitoring CUECs. Some of the user auditors performing financial statement audits replied that they did not rely on the SOC 1 reports and the internal controls described within them due to:

- existing NFRs related to IT controls;
- existing and un-remediated NFRs related to user entities' monitoring of the service organizations' SOC 1 reports and the internal controls described within them; and
- weaknesses in the user entity's internal controls.

As a result of user entities not designing and implementing effective CUECs, user entities and user auditors were not able to rely on SOC 1 reports and the internal controls described within the reports. As discussed earlier, 15 of 30 DoD SOC 1 reports had unmodified opinions, meaning that the service auditor concluded that the service organizations' internal controls described within those reports were designed and operating effectively. However, the IPAs and DoD OIG auditors issued 79 NFRs in FY 2022 related to the design and implementation of CUECs. This indicated that the user entities were not implementing the internal controls that the service organizations described in their SOC 1 reports as being the responsibility of the user entity.

Additionally, in DoD OIG Report No. DODIG-2024-047, "Audit of the DoD's Plan to Address Longstanding Issues with Outdated Financial Management Systems," April 17, 2024, we recommended that the OUSD(C) coordinate with the DoD Chief Information Officer to develop and implement policies and procedures that require DoD Components to document all end-to-end processes relevant to financial transactions with sufficient detail to identify how systems are used. This recommendation will help ensure that CUECs are identified and implemented by the user entities.

To improve the reliability of the SOC 1 reports and the internal controls described within them, the Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, DoD, should develop and implement policies and procedures to coordinate with and hold accountable the user entities to prioritize timely completion of corrective actions on open NFRs related to the design and implementation of CUECs. The Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, DoD, should also identify user entities that are effectively implementing CUECs and identify best practices to help those user entities that are struggling.

The OUSD(C) Should Develop a Feedback Process for SSAE 18 Engagements, Including a Focus on CUECs and User Entities

The OUSD(C) established the FIAR SPWG for service organizations to provide updates on the current SSAE 18 engagements to benefit service organizations, user entities, and auditors in their SSAE 18 engagement and financial statement audits. The FIAR SPWG meets semiannually in May and September. During the meetings the FIAR Directorate provides:

- the progress of current year audits and examinations,
- a template for user entities and auditors to provide feedback on the SOC 1 reports,
- guidance to service organizations on their impact on the user entity's internal controls, and
- CUEC workbooks that include examples of standard internal controls and key supporting documents and data needed to support user auditor testing of CUECs.

Additionally, the service organizations undergoing SSAE 18 engagements provide status updates on the SOC 1 reports to the user entities and user auditors through the FIAR SPWG. The FIAR SPWG discusses any issues found during the ongoing SSAE 18 engagements that may impact financial reporting or audit readiness. Planning efforts by the SPWG and diligence on the role of the service organizations led to unmodified opinions for 15 of 30 SOC 1 reports in FY 2023. While the SPWG has influenced incremental progress, more improvements are needed. During interviews for this management advisory, the service organizations and auditors stated that they found the SPWG meetings beneficial.

However, during one interview, a user auditor suggested that the DoD should annually re-evaluate the meeting dates and attempt to scheduling them to earlier in the year. According to the user auditor, meetings in May are too late for audit planning, and meetings in September are too late in the audit cycle for the user auditors to adjust the scope of internal control and substantive testing because of an unexpected opinion on a SOC 1 report. The DoD OIG agreed with that assessment and, as more DoD agencies get closer to clean audit opinions, shifting planning and internal control testing to earlier in the year will become increasingly important. Therefore, we recommend that the Office of the Under

Secretary of Defense (Comptroller)/Chief Financial Officer, DoD, gather data and feedback from the DoD community, re-evaluate the SPWG dates each year to better align with the financial statement audit planning, testing, and reporting phases, and implement changes as determined appropriate.

Further, there are more than 60 user entities and 50 DoD and commercial service organizations spanning the DoD's SSAE 18 engagements that are not as mature in their financial management processes and need to be prioritized. This will assist the service organizations and user entities in achieving the Department's goal of an unmodified opinion by FY 2028. Therefore, we recommend that the Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, DoD, identify the service organizations that have the biggest impact across the Department and establish specific forums for individual SOC 1 reports that will allow the service organizations to work with user entities and user auditors to discuss SOC 1 report updates, CUECs, and best practices.

Conclusion

Although the DoD spent more than $15.5 million in FY 2023 across 30 SSAE 18 engagements, the IPAs who audit DoD entity financial statements did not always rely on the service organizations' SOC 1 reports and internal controls described within the reports. If the IPAs are unable to rely on the SOC 1 reports and internal controls identified within the reports, efficiencies are lost because the user auditor will perform additional testing, increasing the cost of the financial statement audits and the audit burden on the service organizations and user entities.

Although the DoD has developed a more effective financial management process, communication gaps remain. Until the DoD improves its control environment through more robust communication between service organizations and user entities, and its design, implementation, and monitoring of internal controls over SOC 1 reports and CUECs, there is a risk of:

- user entities not developing and implementing CUECs and improperly relying on service organization internal controls, which may lead to internal control deficiencies not being properly mitigated by user entities;
- the DoD not being able to support the completeness and accuracy of the data processed through DoD IT systems due to unauthorized access, disclosure, and modification to the financial systems and data;
- service organizations providing the MDS and internal controls that may be inaccurate or do not fully reflect the current state of operations; and
- the DoD not being able to obtain an unmodified financial statement opinion at the DoD Agency-Wide level by the congressional mandate of FY 2028.

Recommendation, Management Comments, and Our Response

Recommendation 1

We recommend that the Under Secretary of Defense (Comptroller)/Chief Financial Officer, DoD:

a. Develop and implement policies and procedures to coordinate with, monitor, and hold the user entities accountable for identifying the service organizations which the user entities rely on and develop and implement procedures to communicate with their service organizations, including development of service-level or equivalent agreements that detail roles and responsibilities for each party.

b. Develop and implement policies and procedures to coordinate with and hold accountable the user entities and prioritize timely completion of corrective actions on open recommendations related to the design and implementation of complementary user entity controls required by their service organizations.

Under Secretary of Defense (Comptroller)/Chief Financial Officer, DoD, Comments

The Deputy Chief Financial Officer (DCFO), responding for the USD(C)/CFO, DoD, partially agreed with the recommendations, stating that they agreed with the recommended actions but believed the recommendations should be re-directed to the user entities responsible for:

- identifying and communicating with the service organizations and
- completing corrective actions related to the design and implementation of the CUECs.

The DCFO added that they require the user entities to complete a CUEC Summary Assessment Template twice annually and will continue to coordinate, monitor, and report the status of these recommendations. They provided an estimated completion date of September 2026.

Our Response

Comments from the DCFO did not address the specifics of the recommendations; therefore, the recommendations are unresolved. The USD(C)/CFO is the principal advisor to the Secretary of Defense for all matters related to financial management, including assisting the Components to become audit ready and remediate financial management findings. While we recognize the Components are responsible for identifying and communicating with the service organizations and developing and implementing the CUECs, these recommendations focus on the USD(C)/CFO monitoring and, most importantly, providing assistance and direction to improve the benefits of SSAE 18 engagements. The USD(C)/CFO responses did not address identification of service organizations, communication and agreements between the user entities and service organizations, or completion of corrective actions related to the design and implementation of CUECs. Therefore, we request that the USD(C)/CFO reconsider their position on the recommendations and provide comments within 30 days of the final report.

c. Identify user entities that are effectively implementing complementary user entity controls requirements and share best practices to assist the user entities that need improvement.

Under Secretary of Defense (Comptroller)/Chief Financial Officer, DoD Comments

The DCFO, responding for the USD(C)/CFO, DoD, partially agreed with the recommendation, stating that the OUSD(C) will continue to update the CUEC Workbook annually, which incorporates best practices from user entities that have successfully implemented CUECs. The OUSD(C) also agreed to share controls across DoD from entities that have been successful in implementing controls to address CUECs. They provided an estimated completion date of September 2026.

Our Response

Although the DCFO partially agreed, their planned actions addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once we verify that the information provided and actions taken by the OUSD(C)/CFO, DoD, fully addresses the recommendation.

d. Develop a procedure to gather data and feedback from the DoD financial management and audit communities and re-evaluate the Service Provider Working Group meeting dates each year to ensure user auditors obtain information in time to best plan the financial statement audits to meet planning, testing, and reporting phase timelines, and implement changes as determined appropriate.

Under Secretary of Defense (Comptroller)/Chief Financial Officer, DoD Comments

The DCFO, responding for the USD(C)/CFO, DoD, agreed with the recommendation, stating that the OUSD(C) will re-evaluate the timing of the current SPWG meetings (May and September) and consider a potential third SPWG meeting to support the planning phase of the financial statement audits. The OUSD(C) plans to complete these actions by September 2026.

Our Response

Comments from the DCFO addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once we verify that the information provided and actions taken by the OUSD(C)/CFO, DoD, fully addresses the recommendation.

e. Identify the service organizations that have the biggest impact across the DoD and establish specific forums for the service organizations to work with user entities and user auditors to discuss updates, complementary user entity controls, and best practices to provide continuous improvement toward achieving the congressional mandate of an unmodified financial statement opinion by FY 2028.

Under Secretary of Defense (Comptroller)/Chief Financial Officer, DoD Comments

The DCFO, responding for the USD(C)/CFO, DoD, agreed with the recommendation, stating that the OUSD(C) will coordinate with the financial statement auditors to identify the most impactful SOC 1 reports and determine frequency, timing, and forums with the service organizations, user entities, and their auditors. The OUSD(C) plans to complete these actions by September 2026.

Our Response

Comments from the DCFO addressed the specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once we verify that the information provided and actions taken by the OUSD(C)/CFO, DoD fully addresses the recommendation.

Management Comments

Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, DoD Comments

OFFICE OF THE UNDER SECRETARY OF DEFENSE
1100 DEFENSE PENTAGON
WASHINGTON, DC 20301-1100

October 17, 2024

MEMORANDUM FOR PROGRAM DIRECTOR FOR AUDIT, FINANCIAL MANAGEMENT AND REPORTING, DEPARTMENT OF DEFENSE OFFICE OF INSPECTOR GENERAL

SUBJECT: Response to the Department of Defense Office of Inspector General Draft Report, "Management Advisory: Improvements Needed in the DoD's Planning for and Use of SSAE 18 Engagements" (Project Number D2024-D000FI-0040.000)

The Office of the Under Secretary of Defense (Comptroller) appreciates the Department of Defense (DoD) Office of Inspector General (OIG) for its work on the subject review and the opportunity to review and comment on the draft report dated September 18, 2024.

The essence of the management advisory report is that the Office of the Under Secretary of Defense (Comptroller) should do more in holding the Department's reporting entities accountable for monitoring their service providers and implementing complementary user entity controls (CUECs), while also establishing special forums for financial statement auditors to better understand the scope of System and Organization Controls No. 1 (SOC-1) reports.

During the last five years the Department's internal service providers have achieved unmodified or qualified opinions on their SOC 1 reports at an average rate of 90 percent, and my office has developed and shared helpful tools and templates to implement CUECs. In addition, the Department remains committed to ensuring that CUECs are properly designed and operating effectively.

Accordingly, please find attached a detailed response to the recommendation noted within the draft report. As you will see, I concur or partially concur with each part of the recommendation. My office stands ready to take the actions we describe, and I look forward to our continued engagement on improving the Department as it pursues its goal of an unmodified audit opinion.

Please direct questions regarding this response to [redacted], Staff Accountant, at [redacted] or [redacted].

PIERCE.TINA.MARIE.[redacted]

Tina M. Pierce
Deputy Chief Financial Officer

Attachment:
As stated

Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, DoD Comments (cont'd)

DEPARTMENT OF DEFENSE OFFICE OF INSPECTOR GENERAL
DRAFT REPORT DATED SEPTEMBER 18, 2024
PROJECT NO. D2024-D000FI-0040.000

"MANAGEMENT ADVISORY: IMPROVEMENTS NEEDED IN THE DOD'S PLANNING FOR AND USE OF SSAE 18 ENGAGEMENTS"

OFFICE OF THE UNDER SECRETARY OF DEFENSE (COMPTROLLER) COMMENTS TO THE DOD OFFICE OF INSPECTOR GENERAL RECOMMENDATION

RECOMMENDATION 1.a: We recommend that the Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, DoD: Develop and implement policies and procedures to coordinate with, monitor, and hold the user entities accountable for identifying the service organizations which the user entities rely on and develop and implement procedures to communicate with their service organizations, including development of service-level or equivalent agreements that detail roles and responsibilities for each party.

DoD RESPONSE: Partially concur. Responsibility for identifying and communicating with service organizations, including developing agreements, lies with user entities and service organizations (as acknowledged on page 17 of the Draft Report). This recommendation should be re-directed to the user entities and service organizations. However, the Office of the Under Secretary of Defense (Comptroller) (OUSD(C)) will continue to coordinate, monitor, and report the status to include in governance forums. **Estimated Completion Date September 2026.**

RECOMMENDATION 1.b: We recommend that the Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, DoD: Develop and implement policies and procedures to coordinate with and hold accountable the user entities and prioritize timely completion of corrective actions on open recommendations related to the design and implementation of complementary user entity controls required by their service organizations.

DoD RESPONSE: Partially concur. Responsibility for design and implementation of complementary user entity controls (CUECs), lies with user entities (as acknowledged on page 17 of the Draft Report). This recommendation should be re-directed to the user entities. CUECs have been a Secretary of Defense financial statement audit priority since fiscal year 2022. In addition, OUSD(C) has updated the Statement of Assurance handbook and DoD Internal Control Over Reporting - Financial Reporting and Financial System Guide to require completion of a CUEC Summary Assessment Template twice annually. This template reports status of CUECs Test of Design and Test of Operating Effectiveness. OUSD(C) will continue to coordinate, monitor, and report the status to include in governance forums. **Estimated Completion Date September 2026.**

Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, DoD Comments (cont'd)

RECOMMENDATION 1.c: We recommend that the Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, DoD: Identify user entities that are effectively implementing complementary user entity controls requirements and share best practices to assist the user entities that need improvement.

DoD RESPONSE: Partially concur. OUSD(C) continues to update the CUEC Workbook on an annual basis which includes baseline control descriptions and best practices to address the CUECs. These baseline controls were initially developed utilizing controls from user entities that had implemented controls to effectively address the CUECs. To further assist user entities in addressing the CUECs, OUSD(C) will solicit and make available controls from entities that have been successful in implementing controls to address CUECs. **Estimated Completion Date September 2026.**

RECOMMENDATION 1.d: We recommend that the Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, DoD: Develop a procedure to gather data and feedback from the DoD financial management and audit communities and re-evaluate the Service Provider Working Group meeting dates each year to ensure user auditors obtain information in time to best plan the financial statement audits to meet planning, testing, and reporting phase timelines, and implement changes as determined appropriate.

DoD RESPONSE: Concur. We agree with this recommendation if the auditor community deems adjustments to the current format as being necessary. OUSD(C) currently hosts two Service Provider Working Group Meetings (SPWG), in May and September, that were previously coordinated with user entities, auditors, and service organizations. To further support the financial statement audit-phase timelines, OUSD(C) will re-evaluate the timing of the current two existing SPWG meetings (May and September) and consider a potential third SPWG meeting to support the planning phase of the audit. **Estimated Completion Date September 2026.**

RECOMMENDATION 1.e: We recommend that the Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, DoD: Identify the service organizations that have the biggest impact across the DoD and establish specific forums for the service organizations to work with user entities and user auditors to discuss updates, complementary user entity controls, and best practices to provide continuous improvement toward achieving the Congressional mandate of an unqualified financial statement opinion by FY 2028.

DoD RESPONSE: Concur. OUSD(C) will coordinate with the financial statement auditors to identify the most impactful System and Organization Controls No. 1 (SOC-1) reports and determine frequency, timing, and forum meetings with the service organizations, user entities, and their auditors. **Estimated Completion Date September 2026.**

Whistleblower Protection
U.S. Department of Defense

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible fraud, waste, and abuse in Government programs. For more information, please visit the Whistleblower webpage at www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Reprisal/ or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

For more information about DoD OIG reports or activities, please contact us:

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

www.twitter.com/DoD_IG

LinkedIn
www.linkedin.com/company/dod-inspector-general/

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098