Report No. DOWIG-2026-079

~~CUI~~

INSPECTOR GENERAL

U.S. Department of War

MAY 7, 2026

(U) Audit of Interface Controls Over the DoW's Advancing Analytics Repository

~~Controlled by: DoW OIG~~
~~Controlled by: Audit~~
~~CUI Category: CTI, OPSEC~~
~~Distribution/Dissemination Control: FEDCON~~
~~POC:~~ [redacted]

INDEPENDENCE ★ INTEGRITY ★ EXCELLENCE ★ TRANSPARENCY

~~CUI~~

Pursuant to Executive Order 14347, "Restoring the United States Department of War," September 5, 2025, the Department of Defense Inspector General (DoD IG) and Office of Inspector General (DoD OIG) use the secondary titles of the Department of War Inspector General (DoW IG) and Office of Inspector General (DoW OIG), respectively. The use of these secondary titles does not in any way affect the primary statutory title or authorities of the DoD IG under The Inspector General Act of 1978, as amended (5 U.S.C. Chapter 4, Inspectors General), or the authorities or responsibilities of the DoD IG or DoD OIG pursuant to any laws, regulations, or policies.

(U) Results in Brief

(U) Audit of Interface Controls Over the DoW's Advancing Analytics Repository

May 7, 2026

(U) Objective

(U) The objective of this audit was to assess whether the DoW effectively implemented interface controls to ensure the reliability of data ingested into the Advancing Analytics repository (Advana) from non-financial DoW source systems.

(U) Background

(U) Advana is a DoW-wide data repository that collects, aggregates, and stores large amounts of data from 437 financial and non-financial source systems.

(U) Findings

(U) The Office of the Chief Digital and Artificial Intelligence Officer (OCDAO) did not implement effective interface controls between Advana and non-financial source systems in accordance with requirements from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations." Specifically, the OCDAO did not:

- (U) establish Data Sharing Agreements with 78 of the 387 source systems before establishing a connection to Advana;
- (U) grant privileged access for 26 of 29 privileged users based on accurate and complete access request forms or manage ongoing privileged user access effectively;

(U) Findings (cont'd)

- (U) establish an effective process to monitor user access to Advana;
- (U) implement validation checks to ensure Advana received accurate and complete data from source systems; or
- (U) notify source system owners when an interface error occurred.

(U) According to OCDAO officials, they did not think NIST SP 800-53 requirements were applicable or required for all source systems. In addition, OCDAO officials stated that high staff turnover and shortages contributed to not implementing the controls effectively.

(U) Without effective interface controls, the Chief Digital and Artificial Intelligence Officer (CDAO) has limited assurance that data transferred between source systems and Advana are accurate and complete. Additionally, inaccurate and incomplete data could result in DoW leaders making misinformed decisions affecting DoW operations.

(U) Recommendations

(U) Among the 12 recommendations, we recommended that the CDAO develop and implement interface controls in accordance with NIST SP 800-53 requirements; complete data sharing agreements for systems where such an agreement is not in place; automatically notify system owners when interface errors occur; and implement validation checks for all systems.

(U) Management Comments and Our Response

(U) The Deputy Under Secretary of War for Research and Engineering, responding for the CDAO, agreed with two recommendations and provided planned actions to address them; therefore, those recommendations are resolved but remain open. We will close these recommendations once

(U) Results in Brief

(U) Audit of Interface Controls Over the DoW's Advancing Analytics Repository

(U) Management Comments (cont'd)

(U) we verify that management has implemented corrective actions. The Deputy Under Secretary did not agree with or fully address 10 recommendations presented in the report. Therefore, we request that the CDAO provide comments within 30 days of the final report. Please see the Recommendations Table on the next page for the status of the recommendations.

(U) Recommendations Table

(U) Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Chief Digital and Artificial Intelligence Officer	1.a, 1.b, 1.c, 1.f, 1.g, 1.h, 1.i, 1.j, 1.k, 1.l	1.d, 1.e	None **(U)**

(U) Please provide Management Comments by June 8, 2026.

(U) Note: The following categories are used to describe agency management's comments to individual recommendations.

- **(U) Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **(U) Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **(U) Closed** – The DoW OIG verified that the agreed-upon corrective actions were implemented.


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF WAR

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

May 7, 2026

MEMORANDUM FOR UNDER SECRETARY OF WAR FOR RESEARCH AND ENGINEERING

SUBJECT: (U) Audit of Interface Controls Over the DoW's Advancing Analytics Repository (Report No. DOWIG-2026-079)

(U) This final report provides the results of the DoW Office of Inspector General's audit. 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. These comments are included in the report.

(U) The Deputy Under Secretary of War for Research and Engineering, responding for the Chief Digital and Artificial Intelligence Officer, agreed to address two recommendations presented in the report; therefore, we consider the recommendations resolved and open. We will close these resolved recommendations when you provide us documentation showing that all agreed-upon actions to implement the recommendations are completed.

(U) This report contains 10 recommendations that we consider unresolved because the Deputy Under Secretary of War for Research and Engineering, responding for the Chief Digital and Artificial Intelligence Officer, did not fully address the recommendations presented in the report. Therefore, 10 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.

(U) DoD Instruction 7650.03 requires that recommendations be resolved promptly. For the unresolved recommendations, within 30 days please provide us your response concerning specific actions in process or alternative corrective actions proposed on the unresolved recommendations. For the resolved and open recommendations, please provide us within 90 days your response concerning specific actions in process or completed on the recommendations. Send your response to either [redacted] if unclassified or [redacted] if classified SECRET.

(U) If you have any questions, please contact me at [redacted]. We appreciate the cooperation and assistance received during the audit.

Sean J. Keaney
Acting Assistant Inspector General for Audit
Cyberspace Operations

(U) Contents

(U) Introduction

(U) Objective

(U) The objective of this audit was to assess whether the DoW effectively implemented interface controls to ensure the reliability of data ingested into the Advancing Analytics repository (Advana) from non-financial DoW source systems.[1] See Appendix A for a discussion of the scope and methodology.

(U) Background

(U) The National Defense Authorization Act for FY 2018 required the DoW to develop a data repository to improve data transparency and facilitate DoW-wide analysis and management of business operations.[2] In response to this requirement and with support from private sector partners, the DoW developed Advana. Advana is a DoW-wide data repository that collects, aggregates, and stores large amounts of data—approximately 65.7 petabytes as of May 2025—from 437 financial and non-financial source systems from at least 55 DoW Components and Federal organizations.[3] According to the Office of the Chief Digital Artificial Intelligence Officer (OCDAO) officials, Advana provides DoW military and civilian decision makers with tools and artificial intelligence capabilities to analyze data to make operational decisions.

~~(CUI)~~ Advana was designed to standardize the data it ingests from the source systems into a universal format and separate the data into common DoW business processes, such as financial management, logistics, and readiness and global force management. Advana enables users to search and aggregate data across common business processes to perform analyses and support operational tasks.

[redacted]

[1] (U) This report contains information that has been redacted because it was identified by the Department of War as Controlled Unclassified Information (CUI) that is not releasable to the public. CUI is Government-created or owned unclassified information that allows for, or requires, safeguarding and dissemination controls in accordance with laws, regulations, or Government-wide policies. Our audit focused only on non-financial source systems because Independent Public Accounting firms audit financial source systems during annual financial statement audits. Additionally, an Independent Public Accounting firm specifically audits Advana's interface controls with financial source systems. Unless specified otherwise, the term "source systems" refers only to non-financial source systems.

[2] (U) Public Law 115-91, "National Defense Authorization Act for Fiscal Year 2018", Section 912, "Transparency of Defense Management Data," December 12, 2017.

[3] (U) One petabyte is equal to one million gigabytes.

~~(CUI)~~ [redacted]

(U) Interface Controls

(U) Advana receives data from source systems through an interface, which is a connection that allows systems to exchange information through various methods, such as through cloud services, file transfer protocols, or emails. Interface controls are automated or manual processes designed to ensure accurate, complete, and timely transmission and processing of information between systems (the interface).

(U) DoD Instruction 8510.01, "Risk Management Framework for DoD Systems," requires the DoW to implement interface controls in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 requirements.[4] Although Revision 5 of NIST SP 800-53, issued in September 2020, keeps the requirements of Revision 4 of NIST SP 800-53, it adds eight new security controls that affect interfaces. However, the Deputy DoW Chief Information Officer issued a memorandum on October 16, 2023, authorizing the OCDAO to continue using NIST SP 800-53, Revision 4 requirements for Advana.[5]

(U) Roles and Responsibilities for Managing Interfaces Between Source Systems and Advana

(U) NIST SP 800-53, Revision 4, requires organizations to authorize interfaces between systems using interconnection security agreements.[6] The OCDAO uses Data Sharing Agreements (DSAs), which document the roles and responsibilities for managing interfaces between Advana and the source systems, to meet interconnection security agreement requirements. According to the DSAs, the OCDAO and system owners of interfacing systems are jointly responsible for ensuring data are accurately and completely transmitted in a timely manner.

(U) The OCDAO is responsible for:

- (U) verifying that the data received by Advana are accurately and completely transferred from source systems;
- (U) monitoring the transfer of data from the source systems into Advana;
- (U) notifying source system owners when data transfer errors occur; and
- (U) coordinating with source system owners to correct interface errors.

[4] (U) DoD Instruction 8510.01, "Risk Management Framework for DoD Systems," July 19, 2022.
[5] (U) NIST SP 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013 (including updates as of January 22, 2015). DoD Memorandum, "Adoption of NIST SP 800-53 and CNSSI [Committee on National Security Systems Instruction] 1253 Revision 5," October 16, 2023, authorized Advana to implement NIST SP 800-53, Revision 4 requirements instead of Revision 5 requirements.
[6] (U) NIST SP 800-53, Revision 4, Control CA-03, "System Interconnections," April 2013 (including updates as of January 22, 2015).

(U) Source system owners are responsible for transferring data to Advana in an agreed-upon format, identifying and marking sensitive information, correcting formatting errors, and resubmitting corrected data to Advana through the interface process.

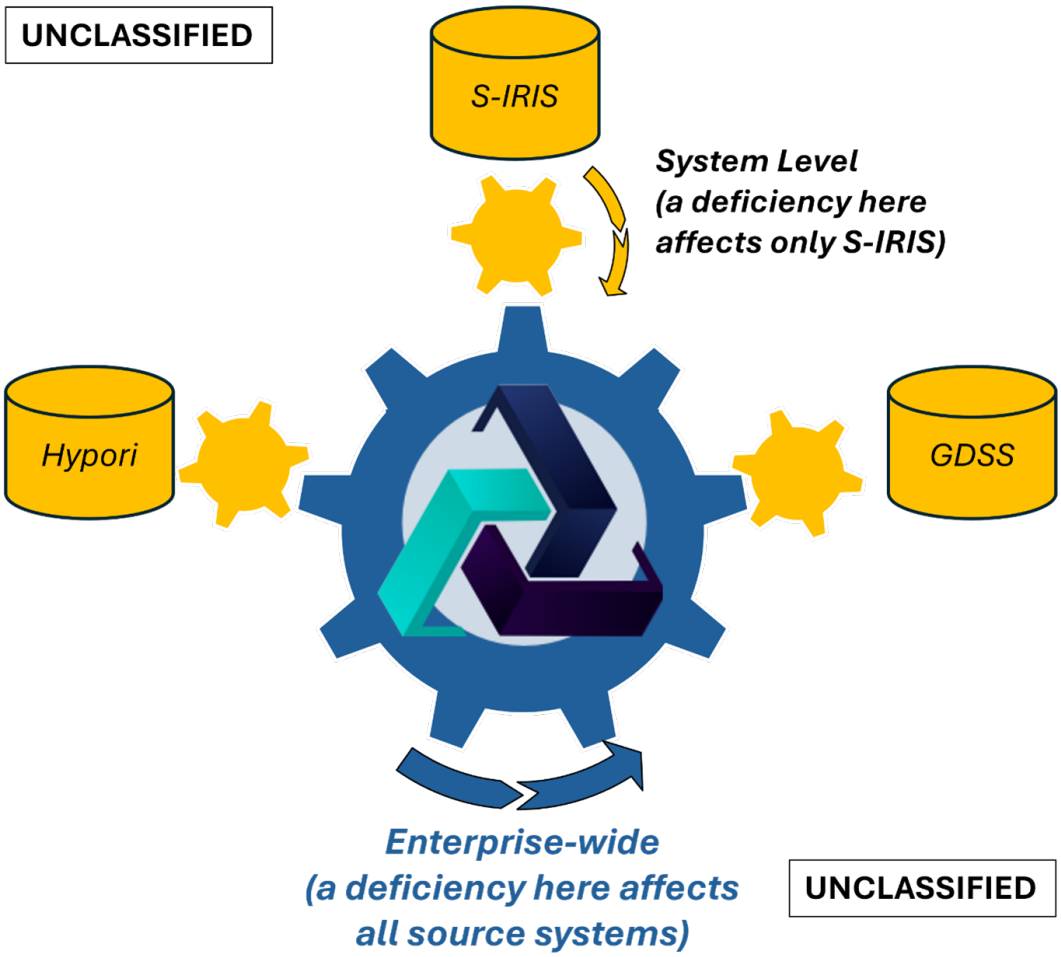
(U) Interface Controls and Systems Reviewed

(U) We assessed the Chief Digital and Artificial Intelligence Officer's (CDAO) implementation of 20 NIST SP 800-53, Revision 4 security controls that we determined were critical to ensuring interfaces between source systems and Advana resulted in accurate, complete, and timely data transmissions between the systems. See Appendix B for the list of controls tested.

(U) For controls implemented uniformly and consistently across all source systems, we evaluated the controls Advana-wide.[7] For example, we assessed the OCDAO's process for managing and monitoring access to Advana. For controls tailored to individual systems, we assessed internal controls for three systems—the Safety-Integrated Risk Information System (S-IRIS); the Hypori Halo (Hypori) platform; and the Global Decision Support System (GDSS). For example, we assessed the OCDAO's process for notifying the three system owners when an error occurred during the interface. Figure 1 shows the distinction between Advana-wide and system-level internal controls.

[7] (U) For this report, "Advana-wide" internal controls are controls that impact all non-financial source systems in a similar manner and may or may not exist or operate similarly for financial systems.

(U) Figure 1. Comparison of Advana-Wide and System-Level Controls



(U) Source: The DoW OIG.

(U) Advana-wide controls are designed and implemented uniformly throughout Advana. However, if not implemented or operating effectively, Advana-wide controls would adversely affect each source system that provides data to Advana equally. Conversely, system-level controls are designed and implemented uniquely for each source system. System-level controls, if not implemented or operating effectively, affect only the source system.

(U) Safety-Integrated Risk Information System

~~(CUI)~~ [redacted]

~~(CUI)~~ [redacted]

(U) Hypori Halo

~~(CUI)~~ [redacted]

(U) Global Decision Support System

~~(CUI)~~ [redacted]

(U) Finding

(U) The OCDAO Did Not Implement Effective Interface Controls for Non-Financial Source Systems Interfacing with Advana

(U) The OCDAO did not implement effective interface controls between source systems and Advana as required by NIST SP 800-53, Revision 4. Specifically, the OCDAO did not:

- (U) establish DSAs with 78 (20 percent) of the 387 source systems before establishing a connection with Advana;[8]
- (U) grant privileged access for 26 (90 percent) of 29 privileged users based on accurate and complete access request forms or manage ongoing privileged user access effectively;
- (U) establish an effective process to monitor user access to Advana;
- (U) implement validation checks to ensure Advana received accurate and complete data from source systems; or
- (U) automatically notify source system owners when an interface error occurred.

(U) According to OCDAO officials, they did not implement these interface controls because they did not think NIST SP 800-53 control requirements were applicable or required for all source systems. In addition, OCDAO officials stated that high staff turnover and staff shortages contributed to not having DSAs in place for all systems and the control weaknesses associated with managing user access.

(U) Advana was developed to improve data transparency and facilitate DoW-wide analysis and management of business operations. Without effective interface controls, the CDAO has limited assurance that data transferred between source systems and Advana were accurate and complete. Additionally, inaccurate and incomplete data in Advana from source systems could result in DoW leaders making misinformed decisions affecting DoW operations, such as those affecting logistics, readiness, and global force management. Although staff for DoW senior leaders identified limited examples in which senior leaders routinely used non-financial data from Advana, decisions, such as those involving munitions and the time to refill stocks, impact DoW-wide operations.

[8] (U) Of the 437 systems that interface with Advana, 387 of them are non-financial systems and 50 are financial management systems that we excluded from the scope of this audit.

(U) The OCDAO Did Not Establish DSAs for All Source Systems Interfacing with Advana

(U) The OCDAO did not establish DSAs with 78 (20 percent) of the 387 source systems before establishing a connection with Advana. NIST SP 800-53, Revision 4, requires organizations to have interconnection security agreements in place before connecting or establishing interfaces between systems. The OCDAO used DSAs to document interconnection security agreement requirements and maintained them in Advana. Although the Advana Data Acquisition Playbook required the OCDAO and system owners to establish DSAs, the OCDAO did not verify DSAs were in place before allowing systems to connect to Advana.[9]

(U) To determine whether a DSA existed for each source system, we downloaded the DSAs in Advana and compared the DSAs to a list of systems interfacing with Advana (provided by the OCDAO). For systems in which we did not find a DSA in Advana, we verified with OCDAO officials that it did not exist.

(U) For the three systems we selected for review, we also verified that the DSAs met the interface interconnection requirements in NIST SP 800-53, Revision 4. The NIST guidance requires organizations to:

- (U) document the interface characteristics, security requirements, and type of information transmitted between systems in the agreement; and
- (U) review the agreement at least annually.

(U) We verified that the OCDAO established DSAs with S-IRIS and Hypori before the systems interfaced with Advana, and we verified that those agreements met NIST requirements. However, the OCDAO did not establish a DSA with GDSS before establishing the system interface with Advana in November 2021.[10] During the audit, the OCDAO established a DSA with the GDSS system owner in October 2024 that met all interconnection security agreement requirements.

(U) By not establishing a DSA, the OCDAO and system owners increase the risk that system owners may not be aware of their responsibilities to document data use restrictions, define applicable data access controls, and ensure all data transmitted or available are accurate and complete. Therefore, we recommend that the CDAO immediately establish DSAs with system owners for the 78 source systems in which an agreement does not exist. In addition, we recommend that the CDAO develop and implement a process to periodically review DSAs to ensure that the agreements comply with NIST SP 800-53 requirements.

[9] (U) The Advana Data Acquisition Playbook, September 30, 2022, outlines the standards for data connections to Advana.

[10] (U) The 78 systems without a DSA with Advana did not include GDSS, because the OCDAO and GDSS system owners established a DSA during the audit.

(U) The OCDAO Did Not Effectively Grant or Manage Privileged Access to Advana

(U) The OCDAO did not grant privileged access for 26 (90 percent) of 29 privileged users based on accurate and complete access request forms or manage ongoing privileged user access effectively. NIST SP 800-53, Revision 4, requires organizations to create and modify accounts in accordance with its defined procedures. The OCDAO's Access Control Policy requires users to submit an approved DD Form 2875, "System Authorization Access Request (SAAR)," or its equivalent, which justifies the need for access.[11] In addition, the policy requires the OCDAO to review the accuracy and completeness of the SAAR form before granting access to Advana.

(U) According to the OCDAO, there were 29 privileged users who could change interface settings or affect the processing of data between Advana and the source systems. We obtained SAAR forms in April 2025 for these 29 privileged users and verified whether the SAAR forms: (1) contained an appropriate justification for access, (2) were appropriately signed, and (3) contained appropriate contract and access expiration information if the SAAR form was for a contractor. We determined that 26 (90 percent) of the 29 SAAR forms reviewed, for one or more reasons, did not support the need for privileged access.[12] Specifically, we found:

- (U) 5 instances in which privileged access was granted despite the SAAR form only supporting general user access;
- (U) 1 instance in which the form did not include a supervisor's confirmation of the user's need-to-know;
- (U) 23 instances in which forms were missing signatures from the supervisor, security manager, or the information owner; and
- (U) 14 instances in which forms for contractors cited access expiration dates that had passed—as far back as May 2019.[13]

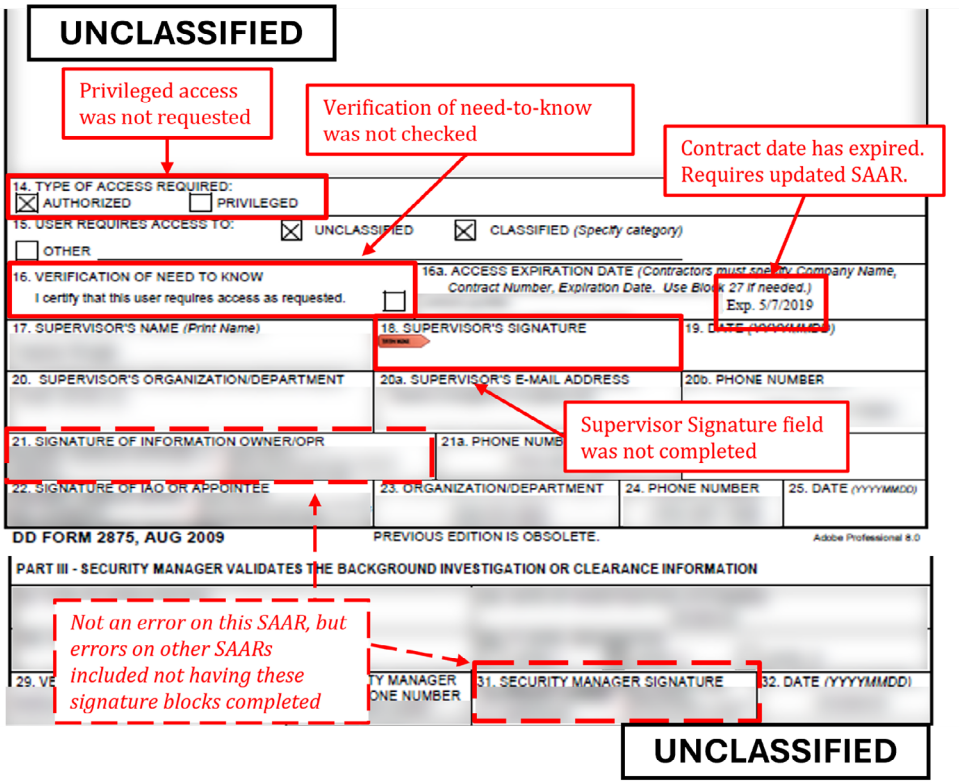
(U) Figure 2 shows an example of an inaccurate and incomplete SAAR form associated with a privileged user's access request that we reviewed.

[11] (U) Chief Digital and Artificial Intelligence Office, "Advana GovCloud Access Control Policy," Version 1.48, November 24, 2023. The System Account Authorization Request (DD Form 2875 or equivalent) is a standard form used within the DoW for requesting and approving access to a system.

[12] (U) The numbers do not sum to 26, because we identified multiple issues on some forms.

[13] (U) We did not test whether these 14 contractors had extended access expiration dates. The contractors may have had a continued need for privileged access, but the SAAR form authorizing privileged access was outdated.

(U) Figure 2. Example of an Inaccurate and Incomplete SAAR Form



(U) Source: The DoW OIG.

(U) Granting privileged access to users, or allowing users to maintain privileged access, with inaccurate and incomplete SAAR forms that lack adequate written justification for privileged access, increases the risk that these users could create security vulnerabilities or make unapproved configuration changes that could cause the interface to fail. Therefore, we recommend that the CDAO review and reconcile users with privileged access to Advana to determine their continued need for privileged access and, based on that review, either remove the user's privileged access or ensure that their SAAR forms are complete and justify the need for privileged access. In addition, we recommend that the CDAO develop and implement procedures to ensure that SAAR forms are processed in accordance with policy requirements.

(U) The OCDAO Did Not Establish an Effective Process to Monitor User Account Access

(U) The OCDAO did not establish an effective process to monitor user account access to Advana. NIST SP 800-53, Revision 4, requires organizations to notify account managers when users no longer need accounts, users are terminated or

(U) transferred, and when a user's need-to-know changes. The CDAO's Access Control Policy identifies two methods for deactivating Advana user accounts when access is no longer needed:

- (U) automatically when accounts are inactive for more than 180 days; or
- (U) manually when receiving a request from the user or the user's supervisor.

(U) However, the Access Control Policy does not include steps to periodically review non-privileged user accounts to ensure that users have a continued need to access data. Therefore, if a deactivation request was not submitted (such as a new supervisor unaware of the user's access), users who no longer have a need-to-know could retain access to Advana by periodically logging into their account, despite no longer requiring such access. Therefore, we recommend that the CDAO update their Access Control Policy to include procedures for periodically reviewing non-privileged user accounts to validate their continued need for access and remove access for users who no longer have a need-to-know for Advana data.

(U) In addition, the Access Control Policy requires the OCDAO to periodically review the continued need for privileged access but does not include steps to verify that contractors with privileged access did not maintain that level of access based on an expired access date. As identified previously in this report, 14 (48 percent) of the 29 SAAR forms that we reviewed showed contractors had access to Advana despite that access being based on an expired access date. By not periodically monitoring contractor account access for such purposes of identifying expired accesses, the OCDAO unnecessarily increases the risk of unauthorized access or data manipulation by privileged users who retain their elevated access when it is no longer required. Therefore, we recommend that the CDAO immediately review and reconcile whether contractors have access to Advana based on expired access dates, and based on that review, remove contractor access for all contractors who no longer require privileged access. In addition, we recommend that the CDAO update their Access Control Policy to require that contractors submit new or updated SAAR forms that identify current access expiration dates. Furthermore, we recommend that the CDAO implement processes to automatically disable contractor accounts when access expires.

(U) The OCDAO Did Not Implement Validation Checks

(U) The OCDAO did not implement validation checks to ensure Advana received accurate and complete data from source systems.[14] NIST SP 800-53, Revision 4, requires organizations to ensure information systems check the validity of organization-defined information inputs, such as character length, acceptable values, and format. Instead, the OCDAO relied on system owners or users of the data to request validation checks or to implement these controls for their systems, despite the CDAO implementing validation checks for financial management systems. For the three systems we selected for review, S-IRIS, GDSS, and Hypori users created their own custom validation checks in the absence of Advana-wide controls to ensure accuracy of data transmitted by these systems.

(U) Implementing validation checks between source systems and Advana would enable the OCDAO to identify and correct inaccurate or incomplete data during data transfers and reduce the risk of DoW leaders making decisions based on unreliable data in Advana. Although the three systems we reviewed implemented validation checks, other system owners and users may not have done the same. Therefore, we recommend that the CDAO, in coordination with system owners, develop and implement validation checks to ensure the accuracy and completeness of data transfers.

(U) The OCDAO Did Not Notify Source System Owners When Interface Errors Occurred

(U) The OCDAO established an automated process to generate error messages when an interface error occurred between Advana and the source systems, but it did not automatically notify source system owners when an interface error occurred. NIST SP 800-53, Revision 4, requires organizations to ensure information systems generate error messages that provide the information necessary for corrective actions.

~~(CUI)~~ Interface errors include incorrect file paths or location and formatting errors. OCDAO personnel stated that the CDAO did not implement this control Advana-wide but instead made source system owners responsible for electing to receive these types of notifications. OCDAO personnel stated that instructions for electing to receive notifications were available online through Advana's Knowledge Base. However, OCDAO personnel did not actively inform system owners of these instructions, and we found, for example, that the [redacted]

[14] (U) We did not validate the completeness and accuracy of the data within the source systems or any information outputs from Advana.

~~(CUI)~~ Relying solely on system owners and users to review Advana's Knowledge Base, without formally notifying them that they must elect to receive error notifications, was ineffective and resulted in at least one source system not receiving notifications that interface errors occurred.

(U) When source system owners are unaware of errors with the interface between their systems and Advana, errors can persist, leading to a disruption in transmitting accurate, complete, and timely data until the error is resolved. Therefore, we recommend that the CDAO automatically notify system owners when an interface error occurs.

(U) Misapplied NIST Standards and Staff Shortages Led to Interface Control Weaknesses or Controls Not Being Implemented

(U) According to the OCDAO, they did not implement interface controls effectively because they did not believe that interface controls between source systems and Advana were required for a large and complicated system like Advana. However, DoD Instruction 8510.01 requires the DoW to implement interface controls in accordance with NIST SP 800-53 requirements, with no exceptions. The Instruction does not exclude systems from this requirement for any reason. In addition, OCDAO officials stated that high staff turnover and staff shortages contributed to not having DSAs in place for all systems and the control weaknesses associated with managing user access.

(U) OCDAO personnel were required to, but did not, implement or effectively implement all NIST SP 800-53 requirements related to interface controls. Implementing these requirements is imperative to ensure that data transfers between source systems and Advana are accurate and complete. If the OCDAO determines, based on a risk assessment, that it is not cost-effective to implement interface controls for every source system, the CDAO should document their decision to not implement the controls for those systems. Therefore, we recommend that the CDAO implement interface controls in accordance with NIST SP 800-53 requirements or, if that is not cost-effective, document the acceptance of risk for not implementing specific controls. In addition, for interface controls not implemented, we recommend that the CDAO notify system owners and users that specific controls were not implemented for specific systems and develop and implement a banner notifying users that the data may be inaccurate or incomplete.

(U) Ineffective Interface Controls Can Lead to Unreliable Data and Misinformed Decisions

(U) The DoW developed and implemented Advana to enhance data transparency across the DoW and enable DoW-wide analysis and management of business operations. The Advana webpage promotes Advana as a reliable source of DoW data.[15] When functioning as intended, Advana provides a crucial foundation for operational and strategic planning, serving as a vital resource for DoW decision makers. However, unimplemented or ineffective interface controls between Advana and its source systems can compromise the data's accuracy and completeness, directly undermining Advana's intended purpose. Furthermore, ineffective interface controls can introduce large-scale inefficiencies across business operations or potentially cause DoW leaders to make misinformed operational or strategic decisions. Although staff for DoW senior leaders identified limited examples in which senior leaders routinely used non-financial data from Advana, decisions, such as those involving munitions and the time to refill stocks, impact DoW-wide operations.

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation 1

(U) We recommend that the Chief Digital and Artificial Intelligence Officer:

a. (U) Immediately establish Data Sharing Agreements with system owners for the 78 source systems for which an agreement does not exist.

(U) Deputy Under Secretary of War for Research and Engineering Comments

(U) The Deputy Under Secretary of War for Research and Engineering, responding for the CDAO, disagreed with the recommendation, stating that the CDAO was attempting to reduce the number of systems requiring DSAs over the next 2 years. The Deputy Under Secretary also stated that the CDAO would only develop DSAs when nonstandard data sharing or governance requirements exist. Additionally, the Deputy Under Secretary stated that the CDAO would review and update their documentation and standard operating procedures to reflect when DSAs were required.

[15] (U) DoW and OCDAO, "About Advana," (No Date Available).

(U) Our Response

(U) Comments from the Deputy Under Secretary did not address all specifics of this recommendation; therefore, the recommendation is unresolved. Removing the requirement to maintain DSAs for all interfacing systems from internal CDAO guidance will not eliminate the responsibility for the CDAO to maintain interconnection security agreements for interfaces between Advana and its source systems in accordance with control CA-03 (System Interconnections) of NIST SP 800-53, Revision 4.

(U) The Advana architecture is complex because it ingests a wide range of nonstandard data (for example, financial, logistical, and health care) from hundreds of source systems with different data protection requirements. To ensure a strong security posture, the CDAO must maintain formal, documented interconnection security agreements with Advana source systems that clearly define roles, responsibilities, interface characteristics, and technical requirements. Having the agreements documented helps as an initial step to supporting the usability of the data, because it reflects the understanding of personnel from both Advana and the source system. Therefore, we request that the CDAO provide comments on the final report describing how they plan to document interface characteristics, security requirements, and responsibilities for the 78 systems without a DSA and how these same requirements will be met if DSAs were required only when nonstandard data sharing or governance requirements exist.

b. (U) Develop and implement a process to periodically review Data Sharing Agreements to ensure that the agreements comply with National Institute of Standards and Technology Special Publication 800-53 requirements.

(U) Deputy Under Secretary of War for Research and Engineering Comments

~~(CUI)~~ [redacted]

(U) Our Response

~~(CUI)~~ Comments from the Deputy Under Secretary did not address all specifics of the recommendation; therefore, the recommendation is unresolved. [redacted]

~~(CUI)~~ [redacted] The CDAO maintains DSAs between Advana and the financial management feeder systems, so it is unclear why the CDAO would not maintain them for non-financial management systems. Therefore, we request that the CDAO provide comments on the final report describing how they plan to periodically review the interconnection security agreements between Advana and the source systems that exchange data.

c. (U) Review and reconcile users with privileged access to Advana to determine their continued need for privileged access, and based on that review, either remove the user's privileged access or ensure that their System Account Authorization Request forms are complete and justify the need for privileged access.

(U) Deputy Under Secretary of War for Research and Engineering Comments

(U) The Deputy Under Secretary of War for Research and Engineering, responding for the CDAO, agreed with the recommendation, stating that the CDAO performed monthly and annual reviews of privileged users and roles as part of Advana's annual System and Organization Controls testing and approved SAAR forms for managing privileged access to the system.[16] The Deputy Under Secretary also stated that activities such as developing code are not privileged user activity. Furthermore, the Deputy Under Secretary stated that Advana had more than 10,000 users who could manage interfaces and that there was a practical limit to their ability to review them all.

[16] (U) An Independent Public Accounting firm audits Advana's interface controls with financial source systems and publishes the results in a System and Organization Controls report.

(U) Our Response

(U) Comments from the Deputy Under Secretary partially addressed the specifics of the recommendation; therefore, the recommendation is unresolved. Although the Deputy Under Secretary stated that the CDAO conducted monthly and annual reviews of privileged user access, as stated in the report, 26 of the 29 SAAR forms for privileged users we reviewed did not support their need for privileged access. We focused on users that were authorized to perform security relevant functions that ordinary users, such as those referred to in the Deputy Under Secretary's comments, were not authorized to perform. Therefore, we request that the CDAO provide comments on the final report describing how they plan to review, reconcile, and update SAAR forms for privileged users requiring privileged access, or remove access for users who no longer require privileged access. We are not recommending SAAR reviews for all users.

d. (U) Develop and implement procedures to ensure that System Account Authorization Request forms are processed in accordance with policy requirements.

(U) Deputy Under Secretary of War for Research and Engineering Comments

(U) The Deputy Under Secretary of War for Research and Engineering, responding for the CDAO, agreed with the recommendation, stating that the CDAO implemented new procedures to automate SAAR form processing.

(U) Our Response

(U) Comments from the Deputy Under Secretary addressed all specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the CDAO provides the updated and approved procedures as well as the documentation supporting the implementation of the automated SAAR form processing procedures.

e. (U) Update their Access Control Policy to include procedures for periodically reviewing non-privileged user accounts to validate their continued need for access and remove access for users who no longer have a need-to-know for data in Advana.

(U) Deputy Under Secretary of War for Research and Engineering Comments

(U) The Deputy Under Secretary of War for Research and Engineering, responding for the CDAO, agreed with the recommendation, stating that the CDAO updated their Access Control Policy.

(U) Our Response

(U) Comments from the Deputy Under Secretary addressed all specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the CDAO provides the updated and approved Access Control Policy, and we verify that it includes procedures for periodically reviewing the non-privileged user accounts.

f. (U) Immediately review and reconcile whether contractors have access to Advana based on expired access dates, and based on that review, remove contractor access for all contractors who no longer require privileged access.

(U) Deputy Under Secretary of War for Research and Engineering Comments

(U) The Deputy Under Secretary of War for Research and Engineering, responding for the CDAO, agreed with the recommendation, stating that the OCDAO reviews its list of privileged users monthly and removes users who no longer require privileged access. The Deputy Under Secretary also stated that implementing Identity, Control, and Access Management requirements in FY 2026 would help to address this recommendation.[17]

(U) Our Response

(U) Comments from the Deputy Under Secretary partially addressed the specifics of the recommendation; therefore, the recommendation is unresolved. Although the Deputy Under Secretary stated that a process was in place, the comments were unclear on whether the process included contractors because the existing Access Control Policy did not address how to manage contractor access. As stated in the report, 14 (48 percent) of the 29 SAAR forms that we reviewed showed contractors continued to have access to Advana despite that access being based on an expired access date on the SAAR form. Therefore, we request that the CDAO provide comments on the final report describing whether the existing process includes contractors and if it does not, the actions the CDAO will take to manage contractor privileged access.

g. (U) Update their Access Control Policy to require that contractors submit new or updated System Account Authorization Request forms that identify current access expiration dates.

[17] (U) Identity, Control, and Access Management is a framework of policies, processes, and technologies designed to ensure that access to information and systems is granted only to authenticated and authorized persons or entities.

(U) Deputy Under Secretary of War for Research and Engineering Comments

(U) The Deputy Under Secretary of War for Research and Engineering, responding for the CDAO, agreed with the recommendation, but stated that the recommendation oversimplified the Access Control Policy. The Deputy Under Secretary stated that Advana's data is sorted into more than 2,000 categories, and the data stewards for each category control their users' access to specific data based on each user's approved role and an active SAAR form on file. The Deputy Under Secretary also stated that the OCDAO regularly reviewed Advana user access and removed access when the SAAR forms on file showed that access had expired.

(U) Our Response

(U) Comments from the Deputy Under Secretary did not address the specifics of the recommendation; therefore, the recommendation is unresolved. The Deputy Under Secretary did not describe how the CDAO would specifically address contractor access or the CDAO's plans to update their Access Control Policy. Therefore, we request that the CDAO provide comments on the final report describing the actions they will take to address contractor access or update their Access Control Policy to improve how they manage contractor access.

h. (U) Implement processes to automatically disable contractor accounts when access expires.

(U) Deputy Under Secretary of War for Research and Engineering Comments

(U) The Deputy Under Secretary of War for Research and Engineering, responding for the CDAO, agreed with the recommendation, stating that the CDAO had a process in place to automatically disable contractor access and would implement a modified version of the process when they implement future Identity, Control, and Access Management requirements.

(U) Our Response

(U) Comments from the Deputy Under Secretary partially addressed the specifics of the recommendation; therefore, the recommendation is unresolved. Although the Deputy Under Secretary stated that a process was in place, the comments were unclear on when that process began. As stated in the report, 14 (48 percent) of the 29 SAAR forms that we reviewed showed contractors had access to Advana despite that access being based on an expired access date on the SAAR form. Therefore, we request that the CDAO provide comments on the final report describing how and when they began automatically disabling expired contractor accounts.

i. (U) Coordinate with system owners to develop and implement validation checks to ensure the accuracy and completeness of data transfers.

(U) Deputy Under Secretary of War for Research and Engineering Comments

(U) The Deputy Under Secretary of War for Research and Engineering, responding for the CDAO, disagreed with the recommendation, stating that Advana was designed to provide flexible data and artificial intelligence tools as well as access to data and the ability for Department users to process data to meet mission requirements. The Deputy Under Secretary stated that system owners, not the CDAO, were responsible for implementing validation checks.

(U) Our Response

(U) Comments from the Deputy Under Secretary did not address all specifics of the recommendation; therefore, the recommendation is unresolved. NIST SP 800-53 requires organizations to validate all incoming data that crosses its authorization boundary.[18] The CDAO, as the Advana platform owner, is responsible for ensuring that validation checks are in place and data hosted on the system conforms to agreed-upon formats and contains acceptable values and character lengths. Therefore, we request that the CDAO provide comments on the final report describing their actions to coordinate with system owners to implement validation checks for data transfers to Advana.

j. (U) Automatically notify system owners when an interface error occurs.

(U) Deputy Under Secretary of War for Research and Engineering Comments

(U) The Deputy Under Secretary of War for Research and Engineering, responding for the CDAO, disagreed with the recommendation, stating that Advana automatically notified those who maintain the interface when or if there is an interface error. The Deputy Under Secretary stated that Advana users were responsible for notifying system owners of data quality issues because most of the connections to source systems were user-controlled.

(U) Our Response

(U) Comments from the Deputy Under Secretary partially addressed the specifics of the recommendation; therefore, the recommendation is unresolved. Although the Deputy Under Secretary stated that Advana automatically notified those who

[18] (U) An authorization boundary includes all components of an information system authorized by an Authorizing Official to operate.

(U) maintain the interfaces, the system owners who are responsible for addressing system interface errors are not automatically notified. The CDAO has a process for system owners to enroll in an automatic notification process; however, as described in the report, system owners were not made aware of that process. An elective process for notifying system owners does not meet NIST SP 800-53 requirements for automatically notifying them. It is imperative that system owners know when an error occurs so that they can assess and take actions to address the error. Therefore, we request that the CDAO provide comments on the final report describing how they plan to automatically notify system owners when interface errors occur.

k. (U) Implement interface controls in accordance with National Institute of Standards and Technology Special Publication 800-53 requirements or, if that is not cost effective, document the acceptance of risk for not implementing specific controls.

(U) Deputy Under Secretary of War for Research and Engineering Comments

(U) The Deputy Under Secretary of War for Research and Engineering, responding for the CDAO, agreed with the recommendation, stating that the CDAO could better inform builders that the data connections are either "transitory" or a "user-controlled connection," which would be subject to NIST SP 800-53 requirements.

(U) Our Response

(U) Comments from the Deputy Under Secretary partially addressed the specifics of the recommendation; therefore, the recommendation is unresolved. Notifying Advana users that they are establishing a user-controlled connection will not address the interface control weaknesses we identified in this report. Our recommendation was specific to the dedicated connections between Advana and the source systems that exchange data and other information resources, not the transitory or user-controlled connections. Therefore, we request that the CDAO provide comments on the final report to clarify how they plan to meet NIST SP 800-53 interface control requirements for the dedicated connections between source systems and Advana.

l. (U) Notify system owners and users that specific controls were not implemented for specific systems, and develop and implement a banner notifying users that the data may be inaccurate or incomplete.

(U) Deputy Under Secretary of War for Research and Engineering Comments

(U) The Deputy Under Secretary of War for Research and Engineering, responding for the CDAO, disagreed with the recommendation, stating that it was beyond the scope of Advana to validate the accuracy or completeness of the data received from source systems. The Deputy Under Secretary also stated that Advana connected to most of the Department's systems and acknowledged that those systems contained inaccurate and incomplete data. In addition, the Deputy Under Secretary stated that ensuring the quality of data in Advana required coordination between the source system data stewards and users instead of a broad, generalized solution.

(U) Our Response

(U) Comments from the Deputy Under Secretary did not address the specifics of the recommendation; therefore, the recommendation is unresolved. The intent of the recommendation was not for the CDAO to validate the accuracy and completeness of source system data. The intent of the recommendation was for Advana to clearly notify users that the data may be inaccurate or incomplete. The Deputy Under Secretary acknowledged the source systems contained inaccurate or incomplete data. However, a user or decision maker may not be aware that the data they are relying on were inaccurate or incomplete. Therefore, we request that the CDAO provide comments on the final report to clarify how they plan to notify Advana users that the data may be inaccurate or incomplete.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this performance audit from July 2024 through November 2025 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

(U) We obtained a universe of 437 financial and non-financial source systems, as of June 2024, from the OCDAO. Of the 437 source systems, we excluded 50 systems from the scope of our audit because they were financial management systems that are audited annually by Independent Public Accounting firms. We assessed 20 controls and identified weaknesses in the design and operating effectiveness of interface controls within Advana. For the 16 controls implemented uniformly and consistently across the remaining 387 non-financial management source systems, we assessed how the OCDAO implemented the controls Advana-wide. For the remaining four controls that involved a system-level component, we assessed internal controls for three systems based on the number of records, number of times users accessed the interfacing system's data, frequency of interfaces, and date the interface with Advana began. The three systems we reviewed were S-IRIS, Hypori, and GDSS.

(U) To understand how the OCDAO and system owners implemented interface controls, we interviewed the OCDAO and system owners from S-IRIS, Hypori, and GDSS. To determine whether the OCDAO implemented interface controls, we:

- (U) reviewed NIST SP 800-53, Revision 4, to understand the requirements for interface controls,
- (U) reviewed policies and procedures related to security and privacy controls, such as the OCDAO's Access Control Policy and Advana Data Acquisition Playbook,
- (U) analyzed DSAs to understand the roles and responsibilities for managing interfaces between Advana and the source systems,
- (U) interviewed OCDAO and source system personnel to understand how interface controls work within Advana, and
- (U) virtually observed how the OCDAO encounters and remediates errors that occur during data transfers through the interface.

(U) To test compliance with NIST SP 800-53, Revision 4 interface requirements, we applied Federal Information System Controls Audit Manual (FISCAM) methodologies because FISCAM includes methodologies designed to assess the effectiveness of interface controls required by NIST SP 800-53, Revision 4.[19] We cross-walked the FISCAM methodologies for interface controls to NIST SP 800-53, Revision 4 requirements, as shown in Table 1.

(U) Table 1. FISCAM to NIST SP 800-53, Revision 4 Cross-walk

(U) FISCAM Interface Control (IN) Activities	Control Activity Description	NIST SP-800-53, Revision 4 Controls Selected*
IN-2.1	Procedures are in place to reasonably assure that the interfaces are accurately and completely processed in a timely manner.	AC-01 AU-01 CA-01 CM-01 MP-01 PL-01 RA-01 SA-01 SC-01 SI-01
IN-2.2	Ownership for interface processing is appropriately assigned.	AC-02 AC-05 AC-06 PL-02
IN-2.3	The interfaced data are reconciled between the source and target application to ensure that the data transfer is accurate and complete.	AC-02* AC-06* CA-03 SA-05 SA-08 SI-10 SI-11 SI-12
IN-2.4	Errors during interface processing are identified by balancing processes and promptly investigated, corrected, and resubmitted for processing.	CA-03* SA-05* SA-08* SI-10* SI-11* SI-12*
IN-2.5	Rejected interface data are isolated, analyzed, and corrected in a timely manner.	SI-10* SI-11* SI-12*
IN-2.6	Data files are not to be processed more than once.	CA-03* SA-05* SA-08*

(U)

(U) * These requirements were tested as part of multiple FISCAM interface control activities.
(U) Source: The DoW OIG.

[19] (U) Government Accountability Office Report GAO-09-232G, "Federal Information System Controls Audit Manual (FISCAM)," February 2009.

(U) Internal Control Assessment and Compliance

(U) We assessed internal controls and compliance with laws and regulations necessary to satisfy the audit objective. In particular, we assessed 20 controls and identified weaknesses in the design and operating effectiveness of interface controls within Advana. However, because our review was limited to these internal control components and underlying principles, it may not have disclosed all internal control weaknesses that may have existed at the time of this audit.

(U) Use of Computer-Processed Data

(U) We used computer-processed data from Advana. The OCDAO exported a list from Advana to Microsoft Excel of all financial and non-financial source systems that interface with Advana, and we used this list to select three source systems to assess the effectiveness of the OCDAO's implementation of system-specific interface controls. We also used this list to verify whether each source system had an existing DSA. In addition to the list of source systems, OCDAO officials provided a log of interface files from Advana for S-IRIS, Hypori, and GDSS that the systems generated between August 2023 and December 2024. We used the computer-processed data to test the OCDAO's implementation of controls. To determine the reliability of the computer-processed data, we observed the OCDAO's generation of the data. We also reviewed the query commands that the OCDAO used to extract the data from Advana to ensure that the data came from a proper source and did not exclude relevant data. Therefore, we concluded that the data we used were sufficient and appropriate to support the audit findings and conclusions.

(U) Prior Coverage

(U) No prior coverage has been conducted on internal controls within Advana for source systems during the last 5 years.

(U) Appendix B

(U) List of Controls Tested

(U) Table 2 identifies the controls we assessed from NIST SP 800-53, Revision 4, which DoW Components are required to follow based on DoD Instruction 8510.01 requirements.

(U) Table 2. Controls, Control Objective, and Results

(U) Control	Control Objectives	Results*
Access Control Family		
AC-01 Access Control Policy and Procedures	This control requires organizations to establish policy and procedures for implementing access controls.	Effective
AC-02 Account Management	This control requires organizations to define procedures to create and manage accounts, decide what roles require privileged access, and monitor these accounts.	Not Effective
AC-05 Separation of Duties	This control requires organizations to define roles and responsibilities for individuals to reduce the risk of suspicious activity without collusion.	Effective
AC-06 Least Privilege	This control requires organizations to allow individuals authorized access only to information necessary to accomplish assigned tasks.	Effective
Audit and Accountability Family		
AU-01 Audit and Accountability Policy and Procedures	This control requires organizations to establish policy and procedures for implementing audit and accountability controls.	Effective
Security Assessment and Authorization Family		
CA-01 Security Assessment and Authorization Policy and Procedures	This control requires organizations to establish policy and procedures for implementing security assessment and authorization controls.	Effective **(U)**

(U) Control	Control Objectives	Results*
CA-03 System Interconnections	This control requires organizations to establish formal agreements to document interface characteristics, security requirements, and annual reviews or updates to the agreement.	Not Effective
Configuration Management Family		
CM-01 Configuration Management Policy and Procedures	This control requires organizations to establish policy and procedures for implementing configuration management controls.	Effective
Media Protection Family		
MP-01 Media Protection Policy and Procedures	This control requires organizations to establish policy and procedures for implementing media protection controls.	Effective
Planning Family		
PL-01 Security Planning Policy and Procedures	This control requires organizations to establish policy and procedures for implementing security planning controls.	Effective
PL-02 System Security Plan	This control requires organizations to establish a system security plan that addresses implemented security controls and control enhancements and describes how the controls meet security requirements.	Effective
Risk Assessment Family		
RA-01 Risk Assessment Policy and Procedures	This control requires organizations to establish policy and procedures for implementing risk assessment controls.	Effective
System and Services Acquisition Family		
SA-01 System and Services Acquisition Policy and Procedures	This control requires organizations to establish policy and procedures for implementing system and services acquisition controls.	Effective **(U)**

(U) Control	Control Objectives	Results*
SA-05 Information System Documentation	This control requires organizations to document implemented security controls to ensure the controls are operating effectively.	Effective
SA-08 Security Engineering Principles	This control requires organizations to implement security engineering principles to new information systems or systems undergoing major changes.	Effective
System and Communications Protection Family		
SC-01 System and Communications Protection Policy and Procedures	This control requires organizations to establish policy and procedures for implementing system and communications controls.	Effective
System and Information Integrity		
SI-01 System and Information Integrity Policy and Procedures	This control requires organizations to establish policy and procedures for implementing system and information integrity controls.	Effective
SI-10 Information Input Validation	This control requires organizations to verify that inputs match specified definitions and content that is transmitted between information systems.	Not Effective
SI-11 Error Handling	This control requires organizations to generate error messages and provide them to the personnel necessary for corrective actions.	Not Effective
SI-12 Information Handling and Retention	This control addresses the handling of information and retention requirements of said information.	Not Effective **(U)**

(U) * We use the terms "effective" and "not effective" to indicate whether a control was in place or we identified weaknesses in the control during testing.

(U) Source: The DoW OIG.

(U) Management Comments

(U) Deputy Under Secretary of War for Research and Engineering

~~CUI~~

RESEARCH AND ENGINEERING

DEPUTY UNDER SECRETARY OF WAR
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

MAR 03 2026

MEMORANDUM FOR DEPARTMENT OF WAR OFFICE OF THE INSPECTOR GENERAL

SUBJECT: Response to Department of War Office of the Inspector General Draft Report, "Audit of Interface Controls Over the Department of Defense's Advancing Analytics Repository"

Attached you will find the Office of the Under Secretary of War for Research and Engineering's official response to the Department of War Office of the Inspector General Draft Report, "Audit of Interface Controls Over the DoD's Advancing Analytics Repository.

For further information, please contact [redacted], who may be reached at [redacted].

James G. Mazol
Deputy Under Secretary of War
for Research and Engineering

Attachment:
As stated

UNCLASSIFIED when separated from CUI document

~~CUI~~

(U) Deputy Under Secretary of War for Research and Engineering (cont'd)

~~CUI~~

Chief Digital and AI Office (CDAO) Response to OIG, "Audit of Interface Controls Over the DoD's Advancing Analytics Repository"

a. (U) Immediately establish Data Sharing Agreements with system owners for the 78 source systems for which an agreement does not exist.

CDAO does not concur with this recommendation; the Advana program is working to significantly reduce the number of systems that we maintain via Data Sharing Agreements (DSAs) with over the next two years and implement DSAs only when nonstandard data sharing or governance requirements exist. The DoW strives to limit the circumstances in which custom data control requirements exist and to pursue a data sharing policy as close to "any authorized user for any authorized purpose as possible". We will carefully review our documentation and SOPs this year to ensure legacy references to a DSA always being required are removed.

b. (U) Develop and implement a process to periodically review Data Sharing Agreements to ensure that the agreements comply with National Institute CA

~~(CUI)~~ [redacted]

c. (U) Review and reconcile users with privileged access to Advana to determine their continued need for privileged access, and based on that review, either remove the user's privileged access or ensure that their System Account Authorization Request forms are complete and justify the need for privileged access.

CDAO concurs and is implementing this recommendation. A majority of interfaces within Advana are built and maintained by writing Python code in Databricks notebooks, which is a builder

~~CUI~~

1
Attachment

(U) Deputy Under Secretary of War for Research and Engineering (cont'd)

~~CUI~~

and developer activity and ***not a privileged user activity.*** Because of this way of operating, the Advana program disagrees with the assessment and interpretation that all interface connections are "privileged user activities." The Advana program does monthly and annual reviews of privileged users and roles which includes reconciliation and the requirement for privileged user access which is part of Advana's annual SOC-1 control testing. There is a practical limit to reviewing the access requests of those who can manage interfaces as that number is in the low 10,000 not the dozen or so NIST envisions for a traditions system interconnection. The Advana program tracks, reviews and approves SAAR forms and actively manages privileged user access.

d. (U) Develop and implement procedures to ensure that System Account Authorization Request forms are processed in accordance with policy requirements.

CDAO concurs with this recommendation and has implemented new procedures to automate SAAR processing ensuring appropriate compliance. The SAARs tested were submitted four years ago and do not reflect the current process implemented since then.

e. (U) Update their Access Control Policy to include procedures for periodically reviewing non-privileged user accounts to validate their (U) continued need for access and remove access for users who no longer have a need-to-know for data in Advana.

CDAO concurs with this recommendation and has updated the Access Control Policy to include appropriate procedures.

f. (U) Immediately review and reconcile whether contractors have access to Advana based on expired access dates, and based on that review, remove contractor access for all contractors who no longer require privileged access.

CDAO concurs and is implementing this recommendation. The list of privileged platform users and access controls are reviewed and updated on a monthly basis. Through this process we are able to identify and rapidly remove any users with expired or unauthorized access to the platform. Additionally, our upcoming implementation of enterprise ICAM (DISA-mandated) in FY26 will also help to further adjudicate and resolve this comment moving into the future. For additional context, ***access of data is not managed at the system-level***, however, we do regularly review access to specific data clusters and data zones. These are reviewed semi-annually by the Advana team and the cluster owners.

g. (U) Update their Access Control Policy to require that contractors submit new or updated System Account Authorization Request forms that identify current access expiration dates.

CDAO concurs in principle with this recommendation, but it is an oversimplification of the access control policy. A large amount of Advana access does not require a SAAR/DD2875 because access controls are managed at the individual data clusters and data zone level (much more granular level.) For context, there are more than ~2,000 data clusters and data zones in the platform today. It is important to note that general access to the Advana platform is not the same as and does not provide access to individual data clusters and data zones automatically. General Advana access control submissions are reviewed regularly; any user with an expired SAARs/DD2875 will

~~CUI~~

2
Attachment

(U) Deputy Under Secretary of War for Research and Engineering (cont'd)

~~CUI~~

have their platform access removed immediately upon review. Data cluster and data zone access is granted through our Service Desk processes, where authorized Advana users (i.e., active SAARs/DD2875s are on file) can request access to specific data clusters and databases that exist within the data zones. Depending on the details of the access request, it will go through multiple levels of reviews/approvals which could include reviews by specific Data Stewards that oversee the use of their organization or system's data on our platform.

h. (U) Implement processes to automatically disable contractor accounts when access expires.

CDAO concurs with this recommendation, is executing on it today and will implement a modified version of it as a part of enterprise ICAM implementation.

i. (U) Coordinate with system owners to develop and implement validation checks to ensure the accuracy and completeness of data transfers.

CDAO does not concur with this recommendation; the intent of the system is designed to provide a flexible set of big data and AI tools to the Department and all DoW users. Advana provides access to data and a means to connect to and process data in order to meet mission requirements (DoW warfighter and business outcomes). Validation checks are not an activity conducted by our platform at the enterprise level as these checks are specific and unique to each data connection established. With this, the responsibility lies with the Advana user responsible for the data connection and pipeline on the platform, and the system owner will typically advise on any validation checks to implement during the initial data acquisition process and development of the data connection, if any are required.

j. (U) Automatically notify system owners when an interface error occurs.

CDAO does not concur with this recommendation; interface errors automatically notify those who manage the interfaces if or when there is an issue. Given the majority of connections to source systems are user-controlled, it is the responsibility of those Advana users to maintain their data connections and inform source system owners if there are impacts within their data pipelines. Additionally, it is the responsibility of source systems owners, and their data stewards, to inform consumers of their data on any changes to their system, or the data it contains, that may have negative downstream impacts around data connection errors or degradation of data quality.

k. (U) Implement interface controls in accordance with National Institute of Standards and Technology Special Publication 800-53 requirements or, if that is not cost effective, document the acceptance of risk for not implementing specific controls.

CDAO concurs with the recommendation of implementing interface controls IAW NIST 800-53. CDAO can better inform builders that the data connections they are building and are maintained in Advana Databricks notebooks would either be considered "transitory" or would be considered a "user-controlled connection" under NIST 800-53.

~~CUI~~

3
Attachment

(U) Deputy Under Secretary of War for Research and Engineering (cont'd)

~~CUI~~

l. (U) Notify system owners and users that specific controls were not implemented for specific systems and develop and implement a banner notifying users that the data may be inaccurate or incomplete.

CDAO does not concur with this recommendation. Advana is connected to the vast majority of major DoW data systems. Given their size and scope, every major DoW data source system contains inaccurate or incomplete data. Assumptions about the scope and mission of the Advana program misinterpret the program charter as a set of available and curated data sets for users to consume. Instead, the charter of the program is to provide the appropriate software tools and platform, in order to enable users across the Department to more easily connect to data, process data, visualize data, access and use discoverable data products via data catalog that are built and maintained by the broader DoW community. Ensuring the consistent quality of data on Advana is not a challenge solved by a broad, generalized solution but requires adequate input and consistent interactions between the source system's data stewards and the Advana users that established the data pipeline on the platform. Specifically, data stewards are looked to as the SMEs for the data they oversee in the source system and have the responsibility to provide the specific data quality rules that should be applied. The Advana users that built the data connection and pipeline on our platform are then responsible for implementing and monitoring the applicable data quality rules, ensuring high confidence in any analytic consumption. Therefore, it is beyond the scope of this program to validate the accuracy or completeness of the upstream data systems that we are receiving data from.

~~CUI~~

4
Attachment

(U) Acronyms and Abbreviations

(U) Advana	Advancing Analytics
(U) CDAO	Chief Digital and Artificial Intelligence Officer
(U) DSA	Data Sharing Agreement
(U) FISCAM	Federal Information System Controls Audit Manual
(U) GDSS	Global Decision Support System
(U) Hypori	Hypori Halo
(U) NIST	National Institute of Standards and Technology
(U) OCDAO	Office of the Chief Digital and Artificial Intelligence Officer
(U) S-IRIS	Safety-Integrated Risk Information System
(U) SAAR	System Account Authorization Request
(U) SP	Special Publication


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF WAR

Whistleblower Protection
U.S. Department of War

Whistleblower Protection safeguards DoW 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 DoW OIG reports or activities, please contact us:

Legislative Affairs Division
legislative.affairs@dodig.mil

Public Affairs Division
public.affairs@dodig.mil

www.dodig.mil

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF WAR OFFICE OF INSPECTOR GENERAL

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