



Inspector General

June 27, 2024

TO: Dr. Colleen Shogan
Archivist of the United States

FROM: Dr. Brett M. Baker
Inspector General

SUBJECT: *Audit of NARA's Information Security Oversight Office*
OIG Audit Report No. 24-AUD-05

The Office of Inspector General (OIG) contracted with Williams Adley & Company-DC, LLP (Williams Adley) to conduct an independent performance audit of NARA's Information Security Oversight Office (ISOO). Attached is Williams Adley's report titled Performance Audit of NARA's Information Security Oversight Office. The objectives of the audit were to 1) determine the effectiveness of ISOO's information security oversight program as it relates to its role of establishing policy and oversight of the government-wide classified national security information (CNSI) system and Controlled Unclassified Information (CUI) during the period of January 1, 2021 through June 30, 2023; and 2) identify best practices and potential improvements to the ISOO's information security oversight program to better achieve its mission. The report contains six recommendations to assist ISOO in its efforts to improve program management and oversight capabilities. Agency staff indicated they had no comments for inclusion in this report.

Williams Adley is responsible for the attached auditor's report dated June 27, 2024 and the conclusions expressed in the report. The findings and conclusions presented in the report are the responsibility of Williams Adley. The OIG's responsibility is to provide adequate oversight of the contractor's work in accordance with Generally Accepted Government Audit Standards.

Please provide planned corrective actions and expected dates to complete the actions for each of the recommendations within 30 days of the date of this report. As with all OIG products, we determine what information is publicly posted on our website from the published report. Consistent with our responsibility under the Inspector General Act of 1978, as amended, we may provide copies of our report to congressional committees oversight responsibility over NARA. We appreciate the cooperation and assistance NARA extended to us during this audit. Please contact me with any questions.

Cc:

William. J. Bosanko, Deputy Archivist of the United States
Merrily Harris, Executive Secretariat
Jay Trainer, Acting Chief Operating Officer and Executive for Agency Services
Micah Cheatham, Chief of Management and Administration
Meghan Guthorn, Deputy Chief Operating Officer
Kevin Pratt, Chief of Staff, Agency Services
William Fischer, Acting Director Information Security Oversight Office
Valerie McMichael, Chief of Staff, Information Security Oversight Office
Kimm Richards, Accountability
William Brown, Senior Program Auditor
Teresa Rogers, Senior Program Auditor
United States Senate Homeland Security and Governmental Affairs Committee
United States House of Representatives Committee on Oversight and Accountability



National Archives and Records Administration

**Performance Audit of NARA's Information Security Oversight Office
(ISOO)**

June 27, 2024





June 27, 2024

Dr. Brett Baker
Inspector General
Office of Inspector General
National Archives and Records Administration

Dear Dr. Baker:

Williams, Adley & Company-DC, LLP was engaged by the National Archives and Records Administration (NARA) Office of Inspector General (OIG) to conduct a performance audit of NARA's Information Security Oversight Office (ISOO). The objectives of our audit are to 1) determine the effectiveness of ISOO's information security oversight program as it relates to its role of establishing policy and oversight of the government-wide classified national security information (CNSI) system and Controlled Unclassified Information (CUI) during the period of January 1, 2021 through June 30, 2023; and 2) identify best practices and potential improvements to the ISOO's information security oversight program to better achieve its mission. We performed the audit in accordance with our Contract No. 88310323A00013, dated July 2, 2023. Our report presents the results of the audit and recommendations to management.

We conducted our audit in accordance with applicable Government Auditing Standards, 2018 revision, technical update April 2021. The audit was a performance audit, as defined by Chapter 8 of the 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 objective.

To accomplish our objectives, we interviewed personnel from NARA's ISOO. We also reviewed documentation related to ISOO procedures for implementing Executive Orders (EO) 13526 "*Classified National Security Information*" and 13556 "*Controlled Unclassified Information*". The scope of the audit was limited to data and processes for the period of January 1, 2021 through June 30, 2023. We conducted fieldwork from October 1, 2023, through March 29, 2024. Appendix 1 provides a more detailed description of our objective, scope, and methodology.

We concluded that although ISOO has policy and oversight functions of the CNSI and CUI programs, certain challenges exist that affect its ability to effectively standardize and assess the management of the programs. Specifically, we noted the following:

- ISOO did not fully document the internal control processes over data collections.
- ISOO does not have a fully defined and documented CNSI Monitoring Methodology.
- ISOO did not fully document the internal control processes over the CUI program.
- ISOO did not carry out all responsibilities of the CUI program executive agent (EA).



These challenges may result in 1) difficulties ensuring all CNSI and CUI agencies are subject to data collections and results are timely, accurately and completely captured in annual reporting; 2) limited ability to support ISOO's current monitoring activities are effective at ensuring agency compliance with the executive orders; and 3) inefficiencies in transitioning monitoring responsibilities to other personnel restricting ISOO's ability to effectively carry out its responsibilities per the executive orders. Therefore, we have made six recommendations to assist ISOO in its efforts to improve program management and oversight capabilities.

We considered internal controls that were significant and relevant to our audit objective and therefore, we may not have identified all the internal control deficiencies with respect to ISOO that existed at the time of this audit. In addition, our work did not include an assessment of the sufficiency of internal control over other matters not specifically outlined in the enclosed report. Williams Adley cautions that projecting the results of our performance audit to future periods is subject to the risks that conditions may materially change from their current status. The information included in this report was obtained from ISOO on or before June 27, 2024. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to June 27, 2024.

We appreciate the opportunity to have conducted this audit. Should you have any questions or need further assistance, please contact us at (202) 371-1397.

A handwritten signature in blue ink that reads 'Leah Southers'.

Leah Southers, CPA, CISA, CGFM, CFE

Partner

Contents

RESULTS IN BRIEF.....	2
BACKGROUND	3
AUDIT RESULTS.....	4
Finding 1: ISOO Should Fully Document Internal Control Processes Over ISOO Data Collections	4
Finding 2: ISOO Does Not Have a Fully Defined and Documented CNSI Monitoring Methodology	5
Finding 3: ISOO Should Fully Document Internal Control Policies Over Controlled Unclassified Information ..	7
Finding 4: ISOO Needs to Strengthen its Compliance with CUI Program Responsibilities	8
APPENDIX 1: OBJECTIVE, SCOPE, AND METHODOLOGY	12
APPENDIX 2: MANAGEMENT RESPONSE	14
APPENDIX 3: ACRONYMS	15
APPENDIX 4: REPORT DISTRIBUTION LIST	16
APPENDIX 5: OIG HOTLINE	17

RESULTS IN BRIEF

Although ISOO has policy and oversight functions of the CNSI and CUI programs, we identified the following four findings that affect its ability to effectively standardize and assess the management of government-wide CNSI and CUI programs through oversight, policy development, guidance, education, and reporting.

Finding 1: ISOO should fully document internal control processes over ISOO Data Collections.

Finding 2: ISOO does not have a fully defined and documented CNSI Monitoring Methodology.

Finding 3: ISOO should fully document internal control policies over CUI.

Finding 4: ISOO needs to strengthen compliance with CUI program responsibilities.

We recommend the Director of ISOO take the following actions:

Recommendation 1: Develop and implement written internal policies and procedures that provide clear guidelines and timelines for data collections.

Recommendation 2: Develop written policies and procedures that detail ISOO personnel responsible for the preparation and review of data collections and a comprehensive list of agencies subject to data collections to ensure CNSI and CUI data collection activities are conducted effectively and uniformly across the office.

Recommendation 3: Formally define and document in writing ISOO's monitoring methodology to address at a minimum program risk, staff responsibilities, and monitoring of program performance.

Recommendation 4: Develop and implement written internal policies and procedures that provide clear guidelines and timelines for CUI program management and oversight processes.

Recommendation 5: Formally document processes in writing that detail ISOO personnel responsible for the preparation and regular review of CUI internal control activities and relevant risks.

Recommendation 6: Develop and document a CUI performance management and oversight plan (i.e., performance measures and controls that ensure compliance with relevant CUI policies and regulations) to address at a minimum staff responsibilities and frequency of activities performed.

BACKGROUND

The National Archives and Records Administration (NARA) is an independent agency of the United States government tasked with preserving and documenting historical government records. NARA also provides guidance to help agencies understand and comply with applicable regulations, executive orders, and the law, in order to support its records management, access, and information security goals. Guidance products are provided to the public and the Federal community in fulfillment of NARA's mission in the areas of Information Security Oversight, Records Management and the grant-making activities of the National Historical Publications and Records Commission (NHPRC).

The Information Security Oversight Office (ISOO) is a component of NARA and is responsible for overseeing the implementation of Executive Order 13526, *Classified National Security Information (CNSI)*, and is the Executive Agent (EA) for oversight of department and agency implementation of controlled unclassified information (CUI) regulations, policies, and procedures under 32 Code of Federal Regulations (CFR) § 2002 "*Controlled Unclassified Information*." In addition, ISOO provides administrative support to the Interagency Security Classification Appeals Panel (ISCAP) and Public Interest Declassification Board (PIDB).

The CNSI program prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. CNSI is information created or received by an agency of the federal government or a government contractor that would damage national security if improperly released. The CUI program represents an initiative to standardize practices across departments and agencies; State, local, Tribal, and private sector entities; academia; and industry. Standardization would enable timely and consistent information sharing and increase transparency throughout the Federal government and with non-Federal stakeholders. CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526. ISOO's role within NARA is to promote the proper classification, protection, and declassification of CNSI and CUI by providing policy guidance and oversight to federal agencies.

The ISCAP acts as an appellate authority for classification challenges, and mandatory declassification requests. The ISOO Director acts as executive secretary for the ISCAP. Established by The Public Interest Declassification Act of 2000, the PIDB advises the President and other executive branch officials on the identification, collection, review for declassification, and release of declassified records and materials of archival value. The ISOO Director serves as executive secretary for the PIDB. ISOO program analysts are assigned to provide administrative support to both ISCAP and PIDB but are not responsible for the effectiveness or outcomes of these programs.

NARA Office of Inspector General (OIG) contracted with Williams, Adley & Company-DC, LLP to conduct a performance audit of ISOO's information security oversight program as it relates to its role of establishing policy and oversight of the government-wide CNSI system and CUI and

identify best practices and potential improvements to the ISOO's information security oversight programs to better achieve its mission. This report describes the results of our audit.

AUDIT RESULTS

ISOO has established policy and oversight functions of the CNSI and CUI programs, and we identified best practices surrounding ISOO's modernization of the data collection process, ISOO's Annual Report to the President, and the Fundamental Classification Guidance Reviews. However, we identified four findings that affect its ability to effectively standardize and assess the management of CNSI and CUI programs. Specifically, we noted the following findings:

Finding 1: ISOO Should Fully Document Internal Control Processes Over ISOO Data Collections

ISOO conducts data collections (also referred to as "data calls") on an annual basis for agencies with CNSI and CUI programs. ISOO did not document in writing the internal controls surrounding the annual CNSI and CUI data collections. Specifically, ISOO did not formally document the process for the identification of agencies to be included in CNSI and CUI data collections or capture the formal procedures and levels of staffing involved, instead ISOO relied on institutional memory and past practices.

ISOO management did not prioritize the development of written internal policies and procedures over CNSI and CUI data collection activities. ISOO management stated due to resource constraints, strategic decisions were made to prioritize the execution of oversight activities.

The lack of documented written policy and procedures can have several detrimental effects on ISOO's data collection process:

- **Accuracy of Annual Reporting to the President:** Without documented policies and procedures, ISOO may face challenges of ensuring all CNSI and CUI agencies are subject to data collections and results are timely, accurately and completely captured in annual reporting.
- **Inconsistent Data Collection Practices:** Without documented policies and procedures, ISOO risks adopting ineffective methods to perform data collections, which may result in inconsistent approaches across CNSI and CUI.
- **Ineffective Contingency Planning:** Without documented policies and procedures, ISOO may face challenges in addressing unexpected resource constraints, such as employee turnover. The inability to effectively transition data collection responsibilities to other personnel could result in ISOO not carrying out its responsibilities per the executive order.

According to Executive Order 13526, "*Classified National Security Information*", 75 Federal

Register 724-725 (December 29, 2009), section 5.2(b)¹ “Under the direction of the Archivist, acting in consultation with the National Security Advisor, the Director of the Information Security Oversight Office shall...(2) oversee agency actions to ensure compliance with this order and its implementing directives.”

While Executive Order 13556², “Controlled Unclassified Information”, 75 Federal. Register 68675 (November 9, 2010), section 2(c) states “The National Archives and Records Administration shall serve as the Executive Agent to implement this order and oversee agency actions to ensure compliance with this order.”

In addition, 32 Code of Federal Regulations § 2002.8 *Roles and Responsibilities* states, the CUI Executive Agent (EA) “Reviews, evaluates, and oversees agencies’ actions to implement the CUI Program, to ensure compliance with the Order, the CFR, and the CUI Registry” and “Reports to the President on implementation of the Order and the requirements of 32 CFR Part 2002. This includes publishing a report on the status of agency implementation at least biennially, or more frequently at the discretion of the CUI EA.”

Further, Government Accountability Office (GAO) Standards for Internal Control in the Federal Government (“Green Book”)³ Principle 12, *Implement Control Activities, Documentation of Responsibilities through Policies* states “Management should implement control activities through policies.”

We recommend the Director of ISOO:

Recommendation 1: develop and implement written internal policies and procedures that provide clear guidelines and timelines for data collections; and

Recommendation 2: develop written policies and procedures that detail ISOO personnel responsible for the preparation and review of data collections and a comprehensive list of agencies subject to data collections to ensure CNSI and CUI data collection activities are conducted effectively and uniformly across the office.

Finding 2: ISOO Does Not Have a Fully Defined and Documented CNSI Monitoring Methodology

ISOO has not documented in writing internal policies and procedures to support its methodology for developing, implementing, and measuring the effectiveness of monitoring activities over

¹ Executive Order 13526 defines what information represents CNSI and standardizes the way the executive branch handles such information. The executive order does not list the universe of agencies and authorized holders subject to the requirements of the order. ISOO must ensure all appropriate entities are subject to CNSI data collections.

² Executive Order 13556 defines what information represents CUI and standardizes the way the executive branch handles such information. The executive order does not list the universe of agencies and authorized holders subject to the requirements of the order. ISOO must ensure all appropriate entities are subject to CUI data collection.

³ GAO-14-704G

agencies with CNSI. Specifically, ISOO's CNSI monitoring methodology has not included: 1) written policies establishing the changes to no on-site visits⁴ and reliance on targeted agency reviews⁵ over agency Security Classification Guides; 2) written procedures documenting the risk considerations and other information evaluated to support the change in monitoring activities, the methodology for performing reviews, the personnel responsible for preparing and reviewing monitoring activities, or the frequency of reviews performed; 3) written guidance supporting ISOO's consideration of external stakeholders⁶ when making determinations on what information should be maintained to support targeted agency reviews performed; and 4) written process to measure the effectiveness of its monitoring activities.

ISOO management did not prioritize the development of written internal policies and procedures over its CNSI monitoring methodology. ISOO management stated due to resource constraints, strategic decisions were made to prioritize the execution of oversight activities.

The lack of a formally defined and documented monitoring methodology may negatively impact ISOO's ability to:

- **Respond to External Requests & Regulatory Oversight:** ISOO cannot timely respond to external requests to support monitoring activities performed.
- **Substantiate Changes to Monitoring Activities:** ISOO lacks documentation to support current monitoring activities are effective at ensuring agency compliance with 32 CFR Part 2001 *Classified National Security Information*.
- **Determine Adequate Resources for the Monitoring Process:** ISOO cannot effectively identify and justify the resources needed, such as human personnel, funding, or technology, to support an effective monitoring function.
- **Define Risks Associated with Monitoring Activities:** ISOO is unable to effectively demonstrate its examination of risks impacting the monitoring process.
- **Ineffective Contingency Planning:** ISOO may face challenges in addressing unexpected resource constraints, such as employee turnover. The inability to effectively transition monitoring responsibilities to other personnel could result in ISOO not carrying out its responsibilities per the executive order.

EO 13526, section 5.2(b) states, "Under the direction of the Archivist, acting in consultation with the National Security Advisor, the Director of the Information Security Oversight Office shall...(4) have the authority to conduct on-site reviews of each agency's program established under this order, and to require of each agency those reports and information and other cooperation that may be necessary to fulfill its responsibilities."

⁴ On-site reviews involve ISOO personnel traveling to agency facilities to perform physical inspections.

⁵ Targeted agency reviews represent a monitoring technique developed by ISOO that focuses on a specific element or activity within an agency's CNSI program.

⁶ ISOO interacts with external parties including regulators, external auditors, other government entities, and the general public.

GAO's Greenbook Principle 7, *Identify, Analyze, and Respond to Risks* states "Management should identify, analyze, and respond to risks related to achieving the defined objectives." In addition, Principle 12, states "Management documents in policies the internal control responsibilities of the organization."

We recommend the Director of ISOO:

Recommendation 3: Formally define and document in writing its monitoring methodology to address at a minimum program risk, staff responsibilities, and monitoring of program performance.

Finding 3: ISOO Should Fully Document Internal Control Policies Over Controlled Unclassified Information

ISOO did not have written documented internal policies and procedures for the control activities performed as the EA for the federal CUI program oversight and performance management. Specifically, ISOO did not have written policies and procedures to support the identification of the agencies subject to the CUI program, activities involved with such identification, timing, and ISOO personnel responsible for performing and reviewing such activities.

ISOO management did not prioritize the development of written internal policies and procedures to support the identification of the agencies subject to the CUI program and related CUI activities. Further, ISOO management stated due to resource constraints, strategic decisions were made to prioritize oversight activities.

The lack of written documented policies and procedures may negatively impact ISOO's ability to:

- **Respond to External Requests & Regulatory Oversight:** ISOO cannot timely respond to external requests regarding CUI activities performed.
- **Substantiate Oversight and Performance Management Activities are Being Performed:** ISOO lacks documentation to support all 12 activities required of CUI EA are being completed and meet the requirements of the Executive Order.
- **Determine Adequate Resources for CUI Processes:** ISOO cannot effectively identify and justify the resources needed, such as personnel, funding, or technology, to support effective oversight or performance management.
- **Define Risks Associated with CUI:** ISOO is unable to effectively demonstrate its examination of risks associated with the CUI oversight and performance management processes in an electronic format suitable to substantiate oversight and performance management processes occur.
- **Ineffective Contingency Planning:** ISOO may face challenges in addressing unexpected resource constraints, such as employee turnover. The inability to effectively transition oversight and performance management responsibilities to other personnel could result in ISOO being unable to fulfill its responsibilities per the executive order.

According to EO 13556⁷, section 2(c), “The National Archives and Records Administration shall serve as the Executive Agent to implement this order and oversee agency actions to ensure compliance with this order.”

In addition, 32 CFR § 2002.2 *Controlled Unclassified Information*, explains that “Executive Agent (EA) is the National Archives and Records Administration (NARA), which implements the executive branch-wide CUI Program and oversees Federal agency actions to comply with the Order. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO).”

Further, Green Book, Principle 7, states that “Management should identify, analyze, and respond to risks related to achieving the defined objectives.” While Principle 12 states “Management documents in policies the internal control responsibilities of the organization”.

We recommend the Director of ISOO:

Recommendation 4: Develop and implement written internal policies and procedures that provide clear guidelines and timelines for CUI program management and oversight processes; and

Recommendation 5: Formally document in writing processes that detail ISOO personnel responsible for the preparation and regular review of CUI internal control activities and relevant risks.

Finding 4: ISOO Needs to Strengthen its Compliance with CUI Program Responsibilities

ISOO experienced challenges fully or actively performing all CUI program responsibilities as the EA per 32 CFR 2002.8. In accordance with GAO’s Standards for Internal Control in the Federal Government, management should identify, analyze, and respond to significant changes that could impact internal controls.⁸ ISOO has not actively performed or fully documented management changes to CUI internal controls for six of the twelve responsibilities of the EA and include:

1. No CUI Advisory Council meetings have been held since June 2022.⁹

⁷ Executive Order 13556 defines what information represents CUI and standardizes the way the executive branch handles such information. The executive order does not list the universe of agencies and authorized holders subject to the requirements of the order. ISOO must ensure all appropriate entities are subject to program management and oversight activities.

⁸ GAO’s Standards for Internal Control in the Federal Government (GAO-14-704G) Principle 9, *Identify, Analyze, and Respond to Change* states “Management should identify, analyze, and respond to significant changes that could impact the internal control system.”

⁹ Per discussion with ISOO management, CUI Advisory Council meetings were halted to participate in the National Security Council’s (NSC) interagency policy committee (IPC) with other CUI stakeholders. On September 7, 2022, ISOO issued CUI Notice 2022-01: *Executive Agent Guidance Regarding White House National Security Council (NSC) Memorandum, “Initiating a Process to Review Information Management and Classification Policies,” June 2, 2022.*

2. No support was provided documenting the timely approval of categories and subcategories of CUI. The last update to categories in the CUI Registry Change Log was September 9, 2022.¹⁰
3. No support was provided documenting the timely review and approval of agency policies implementing the CFR to ensure consistency with the Order, CFR, and the CUI Registry.
4. No updates have been made to the CUI Registry Change Log since September 9, 2022.¹¹
5. Limited support was provided documenting the procedures, guidance, and instructions for oversight and agency self-inspection programs.
6. No support was provided documenting the timely consideration and resolution of disputes, complaints, and suggestions about the CUI Program from entities in or outside the Government.

ISOO management experienced challenges executing the responsibilities of the EA due to resource constraints and the issuance of the White House National Security Council's (NSC) June 2022 memorandum, which fundamentally changed the implementation landscape of the CUI program.¹² This memorandum complicated the EA's responsibilities until the conclusion of the NSC's policy reform process that will lead to a new CUI Executive Order, anticipated in 2024.¹³

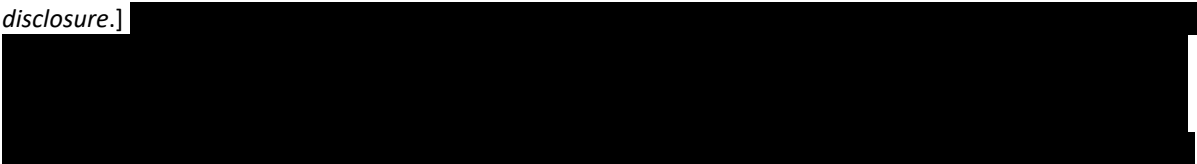
ISOO's impediments surrounding the CUI program, notwithstanding policy reform, may have contributed to challenges in the agencies' implementation of their CUI programs. As of April 9, 2024, ISOO has reported only 40 agencies have implemented CUI policies and only 38 have implemented safeguarding practices.¹⁴ Without stronger management and oversight of the CUI program, it could further delay CUI program implementation, increasing the risk sensitive

ISOO clarified that during the NSC IPC review process, agencies should continue to safeguard and handle CUI in accordance with the applicable federal laws, regulations, and Government-wide policy authorities governing such sensitive information.

¹⁰ [CUI Registry: Change Log | National Archives](#)

¹¹ See Footnote 10.

¹² On June 2, 2022, the NSC issued the memorandum "*Initiating a Process to Review Information Management and Classification Policies*", which established an Information Management and Classification Interagency Policy Committee (IPC) to identify revisions or replacement of Executive Order 13556 "Controlled Unclassified Information." [Note: Due to confidential nature of the NSC memorandum, this content has been redacted for public disclosure.]



However, the memorandum complicated the executive agent's efforts to oversee agency implementation given that some agencies resisted continued coordination and implementation oversight pending resolution of the NSC IPC processes.

¹³ ISOO management stated anticipated concerns surrounding agencies' ability to implement or suspend CUI program efforts were shared with the NSC immediately following issuance of the memorandum.

¹⁴ See ISOO's update on CUI agency implementation efforts in the [ISOO FY 2023 Annual Report](#).

information could be compromised. Specifically, ISOO's difficulties executing all responsibilities of the EA may have several detrimental effects on the CUI program such as:

- Agencies do not have the CUI Advisory Council meetings as a channel to advise the CUI Executive Agent on the development and issuance of policy and implementation guidance for the CUI program.
- Categories and subcategories and the CUI Registry are not updated timely, which may lead to agencies using inaccurate category information in CUI policies.
- Agency CUI policies are not timely reviewed or do not align with the order, CFR, and CUI Registry, which may lead to inaccurate CUI handling and safeguarding practices by agencies.
- Agencies do not have guidance for developing and implementing agency self-inspection programs.
- Disputes, complaints, and suggestions about the CUI Program from entities in or outside the Government are not timely considered or resolved.

According to EO 13556, section 2(c) states "The National Archives and Records Administration shall serve as the Executive Agent to implement this order and oversee agency actions to ensure compliance with this order."

In addition, 32 CFR § 2002.2, explains that "Executive Agent (EA) is the National Archives and Records Administration (NARA), which implements the executive branch-wide CUI Program and oversees Federal agency actions to comply with the Order. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO)."

Further, 32 CFR § 2002.8 "*Roles and responsibilities*" states:

"(a) The CUI EA...(3) Establishes, convenes, and chairs the CUI Advisory Council (the Council) to address matters pertaining to the CUI Program. The CUI EA consults with affected agencies to develop and document the Council's structure and procedures, and submits the details to OMB for approval...

(5) Reviews, evaluates, and oversees agencies' actions to implement the CUI Program, to ensure compliance with the Order, this part, and the CUI Registry...

(7) Approves categories and subcategories of CUI as needed and publishes them in the CUI Registry...

(8) Maintains and updates the CUI Registry as needed...

(9) Prescribes standards, procedures, guidance, and instructions for oversight and agency self-inspection programs, to include performing on-site inspections...

(11) Considers and resolves, as appropriate, disputes, complaints, and suggestions about the CUI Program from entities in or outside the Government..."

Lastly, GAO's Greenbook Principle 7, *Identify, Analyze, and Respond to Risks* states "Management should identify, analyze, and respond to risks related to achieving the defined objectives."

We recommend the Director of ISOO:

Recommendation 6: Develop and document a CUI performance management and oversight plan (i.e., performance measures and controls that ensure compliance with relevant CUI policies and regulations) to address at a minimum staff responsibilities and frequency of activities performed.

APPENDIX 1: OBJECTIVE, SCOPE, AND METHODOLOGY

Audit Objective

The objectives of the audit are to 1) determine the effectiveness of ISOO's information security oversight program as it relates to its role of establishing policy and oversight of the government-wide CNSI system and CUI during the period of January 1, 2021 through June 30, 2023; and 2) identify best practices and potential improvements to the ISOO's information security oversight program to better achieve its mission.

This performance audit was conducted in accordance with Government Auditing Standards, also known as generally accepted government auditing standards, issued by the Comptroller General of the United States ([GAO-21-368G](#)), general and performance audit chapters.

Audit Scope

The scope of the performance audit includes assessing the effectiveness of ISOO during the period of January 1, 2021 through June 30, 2023. In planning and performing our audit, we identified the following control components and underlying principles as significant to the audit objective:

- Control Activities – Design Control Activities and Implement Control Activities
- Risk Assessments – Identify, Analyze, and Respond to Risks

We assessed the design and implementation of these internal controls and identified deficiencies that we believe could affect ISOO's ability to effectively perform program management and oversight functions. The internal control deficiencies we found are discussed in the Audit Results section of this report. However, because our audit was limited to aspects of these internal control components and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

Audit Methodology

During the planning phase, we developed our overall strategy for the expected scope and timing of audit procedures. The planning phase objectives were to develop an understanding of the entity and the objectives of the audit as well as develop testing steps to address the audit objectives.

In the Fieldwork Phase, we obtained sufficient evidence related to the objectives and researchable questions identified in the planning phase. Our fieldwork phase consisted of obtaining an understanding of internal controls related to ISOO's information oversight programs, and testing those controls.

To address our audit objectives, we:

- Conducted interviews with ISOO personnel.

- Performed analysis and evaluation of ISOO's processes related to implementation of identified and relevant criteria affecting the CNSI and CUI programs.
- Performed analysis and evaluation of ISOO's oversight and monitoring of agency activities under EOs 13526 and 13556.
- Performed analysis and evaluation of ISOO's process of data collection and analysis of program performance measures to determine the impact of external and internal changes to the ISOO process.
- Obtained an understanding of ISCAP and PIDB and ISOO's responsibilities for administrative support.
- Evaluated the adequacy and sufficiency of documentation collected.

The purpose of the reporting phase is to report on the results of the audit. Our reporting approach involved an assessment of audit evidence and summary of the results of testing to support audit conclusions.

We conducted this performance audit between July 2023 and March 2024 in accordance with 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.

APPENDIX 2: MANAGEMENT RESPONSE

Agency management stated their general agreement with the findings and recommendations and opted not to provide formal comments for inclusion in this report.

APPENDIX 3: ACRONYMS

Acronym	Definition
NARA	National Archives and Records Administration
ISOO	Information Security Oversight Office
CNSI	Classified National Security Information
CUI	Controlled Unclassified Information
ISCAP	Interagency Security Classification Appeals Panel
PIDB	Public Interest Declassification Board
EA	Executive Agent
CFR	Code of Federal Regulations
GAO	Government Accountability Office
EO	Executive Order
OIG	Office of Inspector General

APPENDIX 4: REPORT DISTRIBUTION LIST

Archivist of the United States

Deputy Archivist of the United States

Acting Chief Operating Officer

Deputy Chief Operating Officer

Chief of Management and Administration

Executive for Agency Services

Chief of Staff, Agency Services

Acting Director, ISOO

Chief of Staff, ISOO

Accountability

United States Senate Homeland Security and Governmental Affairs Committee

United States House of Representatives Committee on Oversight and Accountability

Appendix 5: OIG HOTLINE

The OIG Hotline provides a confidential channel for reporting fraud, waste, abuse and mismanagement to OIG. In addition to receiving telephone calls at a toll-free Hotline number and letters to the Hotline post office box, we also accept emails through an online referral form. Walk-ins are always welcome. Visit <https://naraoig.oversight.gov/> for more information, or contact us:

By telephone

Washington, DC, Metro area: 301-837-3000

Toll-free: 800-786-2551

By facsimile

301-837-3197

By online referral form

<https://naraoig.oversight.gov/online-complaint-form>

Contractor Self-Reporting Hotline

As required by the Federal Acquisition Regulation, a web-based form allows NARA contractors to notify the OIG, in writing, whenever the contractor has credible evidence a principal, employee, agent, or subcontractor of the contractor has committed a violation of the civil False Claims Act or a violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations in connection with the award, performance, or closeout of a contract or any related subcontract. The form can be accessed through the OIG's home page or found directly at <https://naraoig.oversight.gov/oig-contractor-reporting-form>.