



INFORMATION SECURITY OVERSIGHT OFFICE

ISOO

2024
ANNUAL
REPORT

TO THE PRESIDENT OF THE UNITED STATES

Fiscal Year 2024
Annual Report to the President of the United States

August 7, 2025

Information Security Oversight Office
700 Pennsylvania Ave. N.W. Room 100
Washington, DC 20408-0001

Phone: 202-357-5250 | **Fax:** 202-357-5907
Website: www.nara.gov/isoo | **Email:** isoo@nara.gov

LETTER TO THE PRESIDENT

August 7, 2025

The President
The White House
Washington, D.C. 20500

Dear Mr. President,

I am pleased to submit the Information Security Oversight Office's Report for Fiscal Year 2024, as required by Executive Order 13526, "Classified National Security Information," and Executive Order 13556, "Controlled Unclassified Information."

Our government generates and maintains vast amounts of information, put to use every day across America and around the world, for the public good. Much of that information demands special consideration for how it is safeguarded, within and well beyond the confines of government control. The Information Security Oversight Office is singularly positioned to provide insight into the management and health of this unique – and uniquely valuable – national resource, performing an essential role in ensuring that information is both assiduously protected and judiciously shared.

This report, created to support and inform your decision-making on these important issues, provides statistics, analysis, and evaluation of the current state of the Classified National Security Information and Controlled Unclassified Information programs based on the Information Security Oversight Office's review of Departments' and Agencies' self-assessment reporting and our targeted oversight inspections. The report also

includes sections on additional programs and activities that we lead and manage at your direction, including the Interagency Security Classification Appeals Panel, the National Industrial Security Program, and the Public Interest Declassification Board, among others.

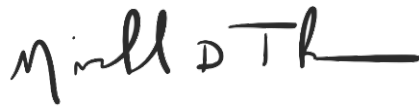
We are in a moment of epochal technological change and to meet this moment our current concepts for information management must evolve. Under your leadership, we must modernize our information security policies, practices, and infrastructure to serve a new landscape of threats, challenges, and opportunities. We must posture our organizations with the capability to move information at the speed of mission, bridging the divide between where our information currently exists – much of it still in paper form – and how it must be managed in order to bring advanced technologies to bear that will enable us to capture its full value. These measures will enable true progress towards resolving longstanding systemic issues of overclassification, infrastructure fragmentation, and the failure to provide ready access to information – issues that simultaneously erode public trust and place our national security at risk.

With your vital action, we can make ready to serve an ever-wider array of potential customers and components of the public interest, while simultaneously ensuring the protection of an ever-larger body of sensitive information that confounds inherited ideas about how to best balance risk and utility. This essential evolution in how we operate will unfortunately remain out of reach without strategic investments in the people, processes, and platforms that bring information to where it is most needed.

The challenge is substantial, to shift the structures – and cultures – of a system that has operated largely unchanged for over seventy years. But it is a challenge that is more than balanced by the scale of the opportunity that awaits us, when we, with your

leadership, unlock the full value of our information, making good on our promise of efficient, effective government, and in so doing, advancing America's security, prosperity, and values.

My team and I have been collaborating closely with members of your National Security Council staff to evaluate and improve the management of both the Classified National Security Information and Controlled Unclassified Information programs. We look forward to realizing and implementing any reforms that you direct.

A handwritten signature in black ink, appearing to read "Michael D. Thomas". The signature is stylized, with the first name "Michael" written in a cursive-like script, followed by "D." and "Thomas" in a more formal, blocky style.

Michael D. Thomas
Director

Table of Contents

LETTER to the PRESIDENT	iii
ABOUT ISOO.....	1
OVERSIGHT and COMPLIANCE.....	5
Oversight of the Classified National Security Information Program.....	5
On-site Inspections	6
Safeguarding of Classified National Security Information Identified Outside of Government Control.....	15
ISOO’s Oversight Of The Controlled Unclassified Information Program.....	17
GUIDANCE and IMPLEMENTATION.....	19
Guidance Issued by ISOO.....	19
Interagency Policy Committee Participation	20
Federal Acquisition Regulation for CUI.....	21
DATA COLLECTION and ANALYSIS	22
Analysis of Department and Agency Expenditures for the CNSI System	22
Original Classification Authority Designations	23
Evaluation of the Declassification-Focused Federal Workforce	24
CUI Program Implementation at Federal Departments and Agencies.....	25
Executive Branch CUI Implementation Status	26
Policy Implementation	27
Physical Safeguarding	29
Information Systems Safeguarding	31
ADMINISTRATION and ENGAGEMENT	35

Support for the Interagency Security Classification Appeals Panel.....	35
ISOO Responsibilities	36
Mandatory Declassification Review Appeals.....	37
Challenges to Classification.....	38
Review of Declassification Guidance	38
Support for the Public Interest Declassification Board.....	38
ISOO Responsibilities	39
Reports and Publications	39
PIDB Meetings and Conferences	39
Administrative Changes	40
Support for the National Industrial Security Program.....	41
ISOO Responsibilities	41
NISP Advances in FY 2024	42
NISP Policy Advisory Committee Activities in FY 2024.....	43
Improving the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information.....	43
ISOO’s Support for State, Local, Tribal, and Private Sector Entity CNSI Programs.....	44
ISOO Responsibilities	44
SLTPS-PAC Activities in FY2024	45



ABOUT ISOO

The notion of an independent government body to oversee the Classified National Security Information System has its modern origins in the Interagency Classification Review Committee (ICRC), established in 1972 by President Richard Nixon with the signing of Executive Order (E. O.) 11652, "Classification and Declassification of National Security Information and Material." The ICRC was composed of representatives from the Departments of Defense, Justice, and State, the predecessor to the Department of Energy, the Atomic Energy Commission, and the Central Intelligence Agency. By 1975, the ICRC's administrative functions had moved from the White House to the National Archives and Records Administration (NARA), then a component of the General Services Administration.

In December 1978, the functions of the ICRC were expanded with the establishment at NARA of the Information Security Oversight Office (ISOO) under President Jimmy Carter. Over the ensuing decades and Presidential Administrations, ISOO's oversight

role in the safeguarding and sharing of America's most sensitive government information, both Classified and Unclassified, has continued to evolve, commensurate with the growing variety, complexity, and quantity of information the government creates, commissions, and securely manages on behalf of our nation.

Today, ISOO leads the government's efforts to assess the management of Classified National Security Information (CNSI) and Controlled Unclassified Information (CUI) through active oversight, the issuing of directives that provide guidance on policy implementation, establishing standards for relevant training, as well as system-wide data gathering and dissemination. Most fundamentally, we support the President by ensuring that the government assiduously protects and judiciously affords access to information that advances the national and public interest. This encompasses a range of ISOO functions, including:

- Developing implementation guidance and approving policies related to the CNSI and CUI programs, under the guidance of the Assistant to the President for National Security Affairs.
- Promulgating standards for: classification, declassification, and marking; safeguarding of classified information; agency security education and training programs; agency self-inspection programs; and classification and declassification guides.
- Serving as Executive Agent to implement and oversee agency actions for the CUI program under [E.O. 13556](#), "Controlled Unclassified Information."
- Conducting robust oversight inspections of federal agencies to vigilantly enforce compliance with Presidential directives such as [E.O. 13526](#), "Classified National Security Information," and to ensure secure handling

and management of CNSI. This includes thorough examination of agency information security training materials, Security Classification Guides (SCGs), marking of classified documents, proper use of Presidential delegated Original Classification Authority (OCA), and agency security management practices.

- Collecting and analyzing information about the status of agency CNSI and CUI programs, and, where necessary, prescribing, after consultation with affected agencies, standardization of forms or procedures.
- Investigating, tracking, and acting on complaints and suggestions from persons within or outside the government with respect to the CNSI and CUI programs and in the instance of a violation, reporting to the head of the agency or to the relevant Senior Agency Official for corrective action, to include requiring that information be declassified by the agency that originated the classification.
- Recommending program changes for the CNSI and CUI programs to the President through the Assistant to the President for National Security Affairs, convening interagency meetings to develop such recommendations.
- Chairing the CUI Advisory Council established under [E.O. 13556](#), the State, Local, Tribal, and Private Sector Policy Advisory Committee under [E.O. 13549](#), "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities," and the National Industrial Security Program Policy Advisory Committee under [E.O. 12829](#), "National Industrial Security Program," as amended.
- Providing programmatic and administrative support for the Interagency

Security Classification Appeals Panel (ISCAP) and the Public Interest
Declassification Board (PIDB).

These activities are summarized in this annual report to the President of the United States, as required under [E.O. 13526, sec 5.2\(b\)\(8\)](#) and [E.O. 13556, sec 5\(c\)](#).



OVERSIGHT and COMPLIANCE

ISOO serves the President and the public as the central governance body for sensitive information created, managed, and maintained by the federal government. This role is enacted via a continuum of authorities and responsibilities encompassing Classified and Unclassified information that exists within and beyond direct government control.

OVERSIGHT OF THE CLASSIFIED NATIONAL SECURITY INFORMATION PROGRAM

The United States government's CNSI program is a uniform system for safeguarding and ensuring appropriate public access to information pertaining to the national defense and foreign relations of the United States that has been determined to require protection against unauthorized disclosure. Information may be classified at one of the

following three levels, which establish discrete standards for its secure management, based on an assessment of the damage to our national security that would result from its unauthorized release:

- “Confidential” information, the unauthorized disclosure of which reasonably could be expected to cause **damage** to the national security;
- “Secret” information, the unauthorized disclosure of which reasonably could be expected to cause **serious damage** to the national security; and
- “Top Secret” information, the unauthorized disclosure of which reasonably could be expected to cause **exceptionally grave damage** to the national security.

Governance of CNSI is broadly defined at the time of this writing by [E.O. 13526](#), “Classified National Security Information,” including specific responsibilities for ISOO and its Director. [Section 5 of E.O. 13526](#) mandates that the Director of ISOO, under the direction of the Archivist and in consultation with the National Security Advisor, shall issue binding directives on executive branch agencies for protecting CNSI and overseeing agency actions to ensure compliance. This includes conducting on-site inspections of agency CNSI programs, with which agencies are required to cooperate.

ON-SITE INSPECTIONS

ISOO conducts robust on-site inspections of executive branch agencies to evaluate the effectiveness of their CNSI programs and to enforce compliance with Presidential directives, such as [E.O. 13526](#). Pursuant to sections [5.2\(b\)\(2\)](#) and [\(4\)](#) of E.O. 13526, we inspect agencies’ CNSI programs with a thorough examination of information security education and training materials, agency SCGs, classification markings on documents, and agency security management practices. ISOO also evaluates whether agencies are

properly utilizing Presidential delegated OCA. Delegations of OCA reported to ISOO in FY 2024 are detailed in the Data Collection and Analysis section of the Annual Report.

ISOO conducted five on-site inspections of federal agencies and examined nine security classification guides over the course of FY 2024. For these inspections, ISOO also instituted multiple improvements to our methodology that have resulted in a more efficient and effective review process, better utilizing ISOO's limited resources to obtain accurate and actionable data on the efficacy of agency CNSI programs, while simultaneously reducing the administrative burden on the agencies being inspected. Improvements instituted in FY 2024 include a data-driven selection methodology for determining which agencies to inspect and the application of a more granular and quantifiable scoring system to establish which areas of agency CNSI programs are performing well and which require further attention. These substantial refinements to our inspection methods, developed and deployed throughout FY 2024, will be fully utilized in ISOO's FY 2025 inspections.

SECURITY CLASSIFICATION GUIDE ASSESSMENTS

SCGs are created and maintained by federal government personnel who have been delegated OCA, as provided for under E.O. 13526 section [2.2\(a\)](#) and 32 CFR Parts [2001.11](#) and [2001.15](#). SCGs are the repository of an organization's decisions, descriptions, and data that explain how to properly classify each agency's unique categories of information to ensure adequate protection. SCGs should clearly indicate the agency's rationale behind these classification decisions and be written in a manner that precludes overclassification or unnecessary limitations to information sharing.

ISOO's periodic reviews of agency SCGs is an essential method of determining the health of an agency's CNSI program. Since 2019, ISOO has employed a standardized

digital scoring rubric to inspect SCGs. ISOO inspectors evaluate each guide in detail, conducting a line-by-line review of the classification decisions and explanatory information within.

In FY 2024, ISOO examined and evaluated nine SCGs from the Department of Commerce, the Department of State, and the Defense Advanced Research Projects Agency (DARPA). Of the SCGs reviewed, two were deficient in listing the appropriate OCA or were not signed, as required under [32 CFR Part 2001.15\(b\)\(2\)](#). Two did not comply with the requirement to list which classification level applies to each element of information, as required under [32 CFR Part 2001.15\(b\)\(6\)](#). One did not properly specify dates or events for declassification, as required under [32 CFR Part 2001.15\(b\)\(9\)](#). Three SCGs did not provide specific reasons for classification or were insufficiently authoritative, placing the weight of decision making on the individual making use of the guide. Unfortunately, all but one of the SCGs reviewed was deficient in some element of the guide requirements listed within [E.O. 13526](#). Deficiencies identified during our review were addressed to the attention of the relevant Senior Agency Official and potential corrective actions were presented by ISOO.

SECURITY EDUCATION AND TRAINING

Effective security training is critical to ensure the proper handling of CNSI by agency employees, limiting security incidents, and protecting national security. ISOO evaluates agency training materials for compliance with 32 CFR Parts [2001.70](#) and [2001.71](#).

In FY 2024, ISOO inspected the training materials of the Departments of Agriculture, Commerce, Interior, the National Geospatial-Intelligence Agency, and the United States Agency for International Development. The most significant trend observed was that agencies have increasingly combined multiple, disparate topics into a single training

module to lessen employee burden. While this consolidation has been satisfactory in some instances, key requirements were missing in others. Another trend observed was the decentralization of training. In two agencies, training was administered by sub-agencies or offices and not tracked in a consolidated manner at the enterprise level.

Of the agencies whose training programs were reviewed by ISOO in FY 2024, three applied the best practice of digital record keeping for training compliance. However, only one agency was found to be proactively removing personnel from access to classified systems if they were found to be non-compliant with training, a requirement of E.O. 13526, sections [1.3\(d\)](#) and [2.1\(d\)](#). Other agencies applied only ad hoc record-keeping methods for security training, such as manually updated spreadsheets, and did not routinely remove non-compliant employees from access.

Initial Employee Training

ISOO inspects initial employee training in accordance with E.O. 13526 section [4.1\(b\)](#) and 32 CFR [2001.70\(b\)](#) and [2001.71\(b\)](#). During ISOO's on-site inspections, we observed a lack of consistency among the topics covered in initial training. One agency's training was missing many of the requirements listed in [32 CFR 2001.71](#). Another agency was not enforcing initial security training for individuals who held a security clearance but were not, at the time, in positions where they would be actively accessing classified information on a regular basis.

Original Classification Authority Training

Training requirements for employees with OCA are explained in 32 CFR Parts [2001.11\(a\)](#) and [2001.70\(c\)](#). This training must be provided upon appointment to a role that includes OCA or a delegation of such authority, and at least annually thereafter. During ISOO's on-site inspections, all agencies had provided initial training for individuals with OCA and could attest to having records of that training. Four agencies

could not provide proof that all individuals had received annual follow-up training. One agency's OCA training was deficient in the elements required for original classification. One agency combined both OCA and derivative classification training into one training, which ISOO assesses might confuse some inexperienced derivative classifiers.

While relatively few individuals, due to highly specialized or senior roles, possess the authority to assess and apply an original classification decision to information, personnel holding a security clearance generally have the lesser authority to derivatively classify information. That is, the ability to summarize, reproduce, or use existing classified information as a source for their communications and production of analysis or other products. Derivative classification training requirements are explained in [32 CFR 2001.71\(d\)](#). In the course of ISOO's on-site inspections, one agency was found not to have specific derivative classification training. However, that agency satisfactorily combined all the required elements of this training into its Annual Refresher Training, which it made mandatory. Another agency's derivative classification training did not have all the required elements pertaining to classification prohibitions specified within E.O. 13526 section [1.7](#).

Annual Refresher Training

All employees who create, process, or handle classified information must receive annual refresher training, as required under [32 CFR 2001.71\(f\)](#). This training should reinforce the policies, principles, and procedures covered in previous training, and cover the identification and handling of other agency-originated information and foreign government information. It should also explain threats and techniques employed by foreign intelligence entities attempting to access classified information and impress upon the employees any and all penalties for engaging in espionage

activities. All of the agencies we reviewed provided training that met these requirements. However, we noted three agencies that lacked an appropriate enforcement mechanism for compliance with the relevant training requirements.

Specialized Security Training

Agencies are required to provide Specialized Security Training to individuals with certain responsibilities under [32 CFR 2001.71\(e\)](#). These positions include classification management officers, security managers, security specialists, declassification authorities, couriers, and other personnel whose duties significantly involve the creation or handling of classified information. Employees are required to take this training within six months of assuming these special duties. One agency inspected had specialized training for most special positions but did not have specific training for its security personnel. Among smaller agencies, this training tends to be explained as “on the job,” handled at the unit level, and not appropriately formalized.

SECURITY PROGRAM MANAGEMENT

Successful implementation of an agency’s CNSI program requires effective program management from its security element(s). ISOO determines if a program is being managed effectively based on an agency’s preparedness, staffing, internal training, perceived senior leadership support for security, record keeping, compliance and enforcement mechanisms, and an examination of how it handles OCA, if applicable. Much of this is determined from the ISOO team’s observations during on-site inspections, including information gleaned from employee interviews. Agencies are additionally evaluated on how prepared they are for ISOO’s on-site inspections.

Staffing and continuity are evaluated based on ISOO’s assessments of whether the security element is properly staffed and organized. ISOO’s recommended practice is for

security offices to develop internal training for their employees. ISOO found that while some agencies require their employees to complete in-house designed training, others encourage staff to take external training from organizations such as the Center for Development of Security Excellence in the Department of Defense.

The health and compliance of agency security programs can vary widely. In ISOO's five on-site inspections during FY 2024, one agency appeared to be notably unprepared for our review. Our inspectors found that this agency ultimately lacked proper resources and management support needed to effectively oversee its CNSI program. A single small team managed the CNSI, Industrial Security, Physical Security, and Controlled Unclassified Information elements. This agency was also plagued by high personnel turnover in its security office.

By contrast, another agency inspected in FY 2024 received high marks across the board, to include significant leadership support for its CNSI program. Our inspectors found that the quality of its internal security office training courses, its meticulous SCGs, and its high-quality searchable database for security-related documents and records were all reflective of ISOO-recommended best practices. Particularly noteworthy was this agency's in-depth, in-person security training for new employees, which exceeded all requirements.

Two agencies inspected in FY 2024 augmented formal compliance requirements with other tools to enhance security awareness, such as: quarterly security newsletters, targeted broadcasts to clearance holders, and security literature such as handouts and bulletins, to enhance security awareness. ISOO reviewers considered these to be best practices for security awareness.

In some instances, agencies whose personnel handle CNSI maintain classification authorities without an apparent, ongoing business need. One agency inspected in FY 2024 had delegated OCA to several individuals who had not made a security classification or declassification decision in over a decade and did not maintain an SCG on behalf of the agency.

Another agency had a compliant SCG, but none of the agency's employees interviewed by ISOO made use of, or were even aware, of the SCG's existence. This same agency had four individuals who had been delegated OCA, but none had made a classification or declassification decision in nearly 15 years. ISOO has observed some agencies which are primarily consumers of CNSI and do not produce originally classified materials have an unnecessarily large number of individuals who have been delegated OCA.

At the systemic level, ISOO assesses that many individuals currently delegated the authority to originally classify information do not need that authority to further their agency's mission.

MARKING OF CLASSIFIED DOCUMENTS

As part of the on-site inspection process, ISOO examines classified documents created by the agency to determine if they are following the proper application of marking and classification requirements listed within E.O. 13526 section [1.6](#) and [32 CFR 2001.20-26](#). ISOO's goal is to review approximately 1% of an agency's self-reported derivatively classified documents, and three to five samples of an agency's originally classified documents (if applicable). This document review serves as a useful indicator to measure the effectiveness of the agency's security training and education program.

Documents are assessed to determine if they have proper overall classification markings and portion markings; whether they are over or under classified; and if they are

properly using Classification Authority Blocks (CABs). Email systems are reviewed to determine if the agency is using a Classification Marking Tool (CMT) to ensure proper classification markings on emails. The integration of a CMT is an ISOO-recommended best practice. Agencies that have not yet implemented such a tool would benefit from incorporating it into their classified email applications. CMTs typically contain prepopulated data for different classification levels and sources from which the authority to classify information is derived, helping a user to apply an accurate classification banner, portion markings, and a CAB to avoid overclassification as well as prevent spillage or incorrect handling by recipients.

Four of the five agencies inspected by ISOO in FY 2024 were primarily customers of other agencies' classified information. As such, these four agencies had few—if any—originally classified documents, but significant numbers of derivatively classified documents. ISOO had a challenging time finding documents to review in our inspections of these agencies. One agency reported creating hundreds of classified documents. However, upon inspection, ISOO determined these were mostly email replies or forwards. Across its five inspections, ISOO reviewed a total of 161 classified documents in FY 2024 and found that 34% contained errors or discrepancies. The most frequent discrepancy was that documents did not include a source list when “multiple sources” were cited. Inspectors also found discrepancies with CABs, including documents having improper duration of classification, improper “classified by” lines, and improper “derived from” lines.

IMPROVEMENTS AND THE WAY FORWARD

For FY 2025, ISOO has developed a new data-driven methodology for determining and prioritizing which agency CNSI programs ISOO should inspect. Original classification authorities, security incidents, agency size, training compliance, and historic ISOO

inspection data are now examined to develop future inspection plans. This methodology more readily identifies programs that may be at risk of noncompliance. This approach also creates a more impartial, impactful, and justifiable selection process. A streamlined on-site inspection standard operating procedure is also being developed, allowing for shorter, more frequent, and more robust inspections. ISOO inspectors will continue to discuss deficiencies with the inspected agency when they are observed, and recommendations will be presented whenever possible to make these inspections more actionable for the agency.

Agency record keeping, such as OCA certification letters, employment termination briefings, non-disclosure agreements, and the status of enforcement mechanisms for non-compliance will also be inspected. Traditionally, the review of agency SCGs was treated as a separate process from on-site inspections, but beginning in FY 2025, the review of agency SCGs will be fully integrated within the on-site inspection process to pursue a more holistic review and provide agencies with a more comprehensive evaluation of their CNSI program.

SAFEGUARDING OF CLASSIFIED NATIONAL SECURITY INFORMATION IDENTIFIED OUTSIDE OF GOVERNMENT CONTROL

Since the implementation of E.O. 13526, ISOO has routinely assisted non-governmental organizations such as universities and state and local archives, as well as private citizens, who find potentially classified information in their possession. [32 CFR Part 2001.36\(b\)](#) provides that: "Anyone who becomes aware of organizations or individuals who possess potentially classified national security information outside of government control must contact the Director of ISOO for guidance and assistance. The Director of ISOO, in consultation with other agencies, as appropriate, will ensure that the safeguarding and declassification requirements of the Order are met."

In FY 2024, ISOO received inquiries from three different non-governmental organizations and one individual reporting the identification of potentially classified material found outside of government control. In all of these instances, records from the reporting entities were transferred to ISOO for safeguarding until they can be properly considered for declassification through the Mandatory Declassification Review (MDR) process provided for under [E.O. 13526](#). Records determined to still contain CNSI following an agency-level equity review will remain in the custody of ISOO until they can be fully declassified.

ISOO's OVERSIGHT OF THE CONTROLLED UNCLASSIFIED INFORMATION PROGRAM

[E.O. 13556](#), “Controlled Unclassified Information,” established the CUI program to standardize the way the executive branch handles unclassified information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that requires safeguarding or dissemination controls pursuant to law, regulation, or government-wide policy. Conceived in the years following the 9/11 attacks to improve interagency information sharing while establishing consistent, standardized handling safeguards to counter growing threats to our sensitive, unclassified information and systems, the E.O. designated NARA as the Executive Agent for the program, executing these responsibilities through the Director of ISOO.

[32 CFR 2002](#) implemented the CUI program requirements for safeguarding, disseminating, marking, decontrolling, and disposing of CUI and also established responsibilities of the CUI Executive Agent, including ISOO's responsibility for implementing the CUI program within the executive branch and overseeing federal agency actions to comply with [E.O. 13556](#).

ISOO oversees agencies' implementation of the CUI Program, pursuant to sections [2\(c\)](#) and [5\(b\)](#) of E.O. 13556. ISOO initially established deadlines for phased implementation of the CUI Program at the agency level, while [CUI Notice 2020-01](#) identified separate implementation deadlines for key areas of program implementation: policy, physical safeguarding, and information systems safeguarding.

Since the issuance of [E.O. 13556](#), there have been continued gains in implementing CUI across the federal government. Based on data collected annually from agencies by ISOO, as of the conclusion of FY 2024, approximately half of federal agencies have

completed and implemented their CUI policy. Additionally, nearly three quarters of agencies have begun acquiring the funding and resources they need to fully implement their programs. More granular information on agency-level CUI information is provided in the Data Analysis and Reporting section of the ISOO Annual Report.



GUIDANCE and IMPLEMENTATION

ISOO's oversight of the CNSI and CUI programs entails the regular issuance of, and participation in, interagency processes designed to produce, policy and implementation guidance that support the successful and legally compliant execution of these programs at the agency level.

GUIDANCE ISSUED BY ISOO

Pursuant to ISOO's authorities under [E.O. 13526](#), ISOO issued three Notices in FY 2024. ISOO Notices are binding directives, issued under the direction of the Archivist and in consultation with the National Security Advisor, which serve as a means of providing clarifying guidance stemming from existing statutory, regulatory, or executive order requirements or mandates.

[ISOO Notice 2024-01](#), “Joint Ventures and Entity Eligibility Determinations”, a joint Notice issued in tandem with the Small Business Administration (SBA), provides guidance on entity eligibility determinations, sometimes referred to as “facility security clearances” for joint ventures in the NISP. The need for clarification arose in light of an SBA rule (Oct. 16, 2020), which addressed joint ventures under the SBA’s programs, and a subsequent Government Accountability Office decision (August 27, 2021) that interpreted the SBA rule without addressing NISP requirements and [32 CFR part 2004](#) or how the two interconnect, thus adding to the confusion. ISOO received requests for clarification from several agencies, and this Notice provides agencies with guidance clarifying how the SBA regulations interact with NISP requirements.

[ISOO Notice 2024-02](#), “Agencies Eligible to Receive Referrals from Automatic Declassification at 25, 50, and 75 Years” was issued to convey publicly those agencies that received approval from the ISCAP to exempt specific information from automatic declassification and that are authorized to receive referrals resulting from automatic declassification reviews. Agencies are limited to exempting from automatic declassification only those approved exemptions listed in the tables in that Notice.

[ISOO Notice 2024-03](#), “Changes to ISOO Liaison Program” was issued to announce changes to ISOO liaison program, which is the office’s primary formal mechanism of engaging with federal agencies on their CNSI programs. The notice established a single ISOO liaison e-mail box and streamlined the way ISOO engages with its interagency liaisons to more efficiently oversee the CNSI program.

INTERAGENCY POLICY COMMITTEE PARTICIPATION

On June 2, 2022, the National Security Council (NSC) Staff issued a memorandum to agencies which aimed to overhaul, update, and streamline the many ways that the

executive branch creates and manages classified and controlled unclassified information, including special access programs (SAPs).

Throughout 2024 ISOO continued to support NSC-led inter-agency policy processes to update and reform the CUI and CNSI programs. While these processes identified some important improvements, they did not result in the publication of new policies. ISOO supports the continued oversight of these programs and is always willing to engage in policy processes to improve and modernize program compliance and security.

FEDERAL ACQUISITION REGULATION FOR CUI

The General Services Administration has reported that the Office of Federal Procurement Policy has completed its review of the Federal Acquisition Regulation's CUI clause. The rule was resubmitted to OMB's Office of Information and Regulatory Affairs and is currently undergoing the standard process for interagency review.

This clause is a key element in how agencies will implement CUI. Once issued, this regulation will help standardize the way executive branch agencies enforce the requirements of the CUI framework with nonfederal entities that receive CUI.



DATA COLLECTION and ANALYSIS

Pursuant to E.O. 13526 sections [5.2\(b\)\(2\)](#) and [\(4\)](#), E.O. 13556 sections [2c](#) and [5c](#), 32 CFR Parts [2001.90\(b\)](#), and [32 CFR 2002.8\(c\)\(6\)](#), agencies report to ISOO data related to their CNSI and CUI programs. This information is gathered through an annual data call, used to generate statistics and analysis to inform ISOO's oversight team on areas of focus as they conduct inspections, as well as our annual report.

ANALYSIS OF DEPARTMENT AND AGENCY EXPENDITURES FOR THE CNSI SYSTEM

ISOO collects several cost-related data elements for the CNSI system on an annual basis under [E.O. 13526 section 5.4\(d\)\(8\)](#) and [32 CFR 2001.90\(c\)](#). This cost data has fluctuated significantly year-over-year, making it challenging to draw reliable conclusions at either

the agency or system level based on this information. One example of this dynamic is found in the data agencies annually report to ISOO on the costs of their CNSI security clearance investigations and reinvestigations.

For FY 2021, agencies reported a total of \$1.5 billion in expenditures in this area. For FY 2022, those same agencies reported approximately \$714 million, less than half of the amount reported in the preceding year. In the next fiscal year, FY 2023, the reported total for the same question was approximately \$300 million, another apparent drop of more than 50% in agency spending in this area from the preceding year. It is unclear based on the information currently available to ISOO whether these significant fluctuations are a product of varying methods of accounting for the funds in question or if they represent a true and dramatic drop in agency expenditures.

For FY 2024, the total amount reported by agencies for security clearance investigations was reported to ISOO as just over \$983 million, indicating a greater than 200% increase over the amount reported for FY 2023.

ORIGINAL CLASSIFICATION AUTHORITY DESIGNATIONS

Original classification refers to an initial determination about the appropriate level of protection that is warranted for information, based on a determination of the reasonable expectation of damage to U.S. national security that would result from the unauthorized disclosure of that information, as defined in [E.O. 13526](#). This authority to originally classify information, referred to as OCA, may be exercised only by the President, the Vice President, those officials designated by the President, and any officials delegated this authority pursuant to procedures set forth in [E.O. 13526](#). Such original classification decisions are documented, with supporting information, in

agency SCGs to aid in the accurate classification of information throughout and across organizations.

Agencies that manage classified information often have specific individuals who have been delegated OCA. These individuals bear organizational responsibility for the maintenance of SCGs, among other specialized functions relating to classification and declassification. Consistent with [E.O. 13526](#), delegations of OCA must be limited to the minimum required to administer the CNSI program. Agency heads are responsible for ensuring that designated subordinate officials who are delegated this authority have a demonstrable and continuing need to exercise it. [E.O. 13526](#) requires agencies to report OCA delegations to the Director of ISOO.

In FY 2024, 19 agencies reported the following 1,661 OCA delegations:

- 694 Top Secret-level OCAs
- 963 Secret-level OCAs
- 4 Confidential-level OCAs

EVALUATION OF THE DECLASSIFICATION-FOCUSED FEDERAL WORKFORCE

ISOO also collects annual data from agencies with declassification programs to document the number of full-time equivalent (FTE) employees in these organizations that have declassification as a primary duty. The total number of declassification-focused FTE employees reported for FY 2024 was 1,384. ISOO tracks declassification-focused personnel across twelve discrete areas. These twelve areas, and the number of associated personnel, are listed below. Because FTE employees are calculated based on hours worked, rather than personnel, the figures provided by agencies were often

represented as fractions. As a result, the numbers in the table below have been rounded to present whole numbers.

Declassification Activity	Number of FTE
Automatic Declassification	390
Systematic Declassification	45
Ad Hoc Declassification	48
Prepublication Review	58
Court-Related Declassification	72
NATO / International Use	16
Freedom of Information Requests	539
Mandatory Declassification Review	97
ISCAP Declassifications	23
Declassification by Law or Regulation	38
Congressional-Related Action	19
Foreign Relations of the United States	39

ISOO also gathered data from agencies on how many FTE employees are devoted to agency CNSI self-inspection programs. The total number reported to be working in this area across the federal government was 649.

CUI PROGRAM IMPLEMENTATION AT FEDERAL DEPARTMENTS AND AGENCIES

The CUI program is intended to standardize the way the executive branch handles unclassified information that requires safeguarding or dissemination controls. Prior to implementation of the CUI Program, agencies employed ad hoc, agency-specific

policies, procedures, and markings to safeguard and control this information, such as information that involves privacy, security, proprietary business interests, and law enforcement investigations. This contributed to persistent government-wide information management problems that included inconsistent marking and safeguarding of documents from agency to agency, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing. While the CUI program has not yet resolved all of these issues, ISOO assesses that the program’s full implementation across the federal government is an important step towards doing so.

EXECUTIVE BRANCH CUI IMPLEMENTATION STATUS

Each year, as part of its annual data call, ISOO requests information from federal agencies related to the status of their CUI program implementation. Specifically, ISOO asks questions to determine whether the agency has developed an internal CUI policy to implement the CUI program, established physical safeguarding requirements, and implemented information systems safeguards. ISOO has focused on the implementation efforts of 15 cabinet-level departments and 67 other independent agencies. The chart below indicates the percentage of agencies that have completed the three critical CUI implementation requirements, the percentage of agencies that have begun but were pending completion at the end of FY 2024, and those that are currently non-compliant with that CUI program requirement.

	Complete	Pending	Non-Compliant
Agency CUI Policy	50%	45%	5%
Physical Security	51%	44%	5%
Information Systems	41%	54%	5%

POLICY IMPLEMENTATION

[CUI Notice 2020-01](#) established a deadline for agencies to issue policy to implement the CUI Program by December 31, 2020. The onset agency closures and varying working arrangements resulting from the COVID-19 pandemic significantly hampered policy development at the agency level. Thereafter, in June 2022, the National Security Council initiated an Information Management and Classification Interagency Policy Committee (IPC) to consider revising or replacing E.O. 13556, which led many agencies to pause or slow CUI implementation in anticipation of new guidance.

The status of agency CUI policies at the end of FY 2024 is indicated in the chart below, based on self-reporting, including projected dates for implementation as provided by agencies.

Agency	CUI Policy Status
Ability One Commission	Complete
Administrative Conference of the U.S.	9/30/2025
Advisory Council on Historic Preservation	Complete
Barry Goldwater Scholarship and Excellence in Education Foundation	Complete
Central Intelligence Agency	12/31/2026
Commission of Fine Arts	Not Started
Commission on Civil Rights	11/3/2026
Commodity Futures Trading Commission	9/30/2025
Consumer Financial Protection Bureau	6/1/2025
Consumer Product Safety Commission	12/31/2024
Defense Nuclear Facilities Safety Board	Complete
Denali Commission	12/31/2025
Department of Agriculture	9/30/2025
Department of Commerce	Complete
Department of Defense	Complete
Department of Education	Complete
Department of Energy	Complete
Department of Health and Human Services	12/31/2024
Department of Homeland Security	Complete
Department of Housing and Urban Development	4/1/2025

Department of Interior	Complete
Department of Justice	Complete
Department of Labor	Complete
Department of State	4/30/2025
Department of Transportation	Complete
Department of Treasury	Complete
Department of Veterans Affairs	Complete
Environmental Protection Agency	Complete
Export-Import Bank of the U.S.	Complete
Farm Credit Administration	Complete
Federal Communications Commission	2/28/2025
Federal Election Commission	9/30/2025
Federal Energy Regulatory Commission	Complete
Federal Housing Finance Agency	Complete
Federal Labor Relations Authority	Complete
Federal Maritime Commission	Complete
Federal Mediation and Conciliation Service	Complete
Federal Mine Safety and Health Review Commission	6/30/2025
Federal Retirement Thrift Investment Board	Complete
Federal Trade Commission	Complete
General Services Administration	Complete
Institute of Museum and Library Services	12/30/2025
Inter-American Foundation	Complete
International Development Finance Corporation	12/31/2024
James Madison Memorial Fellowship Foundation	3/1/2025
Marine Mammal Commission	12/31/2025
Merit Systems Protection Board	10/1/2025
Millennium Challenge Corporation	Complete
Morris K. Udall and Stewart L. Udall Foundation	9/30/2026
National Aeronautics and Space Administration	Complete
National Archives and Records Administration	1/1/2026
National Capital Planning Commission	9/30/2025
National Council on Disability	2/28/2025
National Credit Union Administration	Complete
National Endowment of the Arts	Complete
National Labor Relations Board	Complete
National Mediation Board	12/31/2025
National Science Foundation	Complete
National Transportation Safety Board	Complete
Nuclear Regulatory Commission	Complete
Nuclear Waste Technical Review Board	9/30/2025
Occupational Safety and Health Review Commission	3/31/2025
Office of Government Ethics	Complete
Office of Personnel Management	9/30/2025

Office of Special Counsel	Did Not Report
Office of the Director of National Intelligence	12/31/2029
Pension Benefit Guaranty Corporation	12/31/2024
Postal Regulatory Commission	12/30/2024
Railroad Retirement Board	12/31/2025
Securities and Exchange Commission	12/30/2025
Selective Service System	Complete
Small Business Administration	Complete
Social Service Administration	Complete
Surface Transportation Board	Complete
Tennessee Valley Authority	12/30/2025
Trade and Development Agency	6/30/2025
U.S. Access Board	12/31/2025
U.S. African Development Foundation	Did Not Report
U.S. Agency for Global Media	5/25/2025
U.S. Agency for International Development	1/31/2025
U.S. Interagency Council on Homelessness	Not Started
U.S. International Trade Commission	Complete

PHYSICAL SAFEGUARDING

In accordance with various laws, regulations and government-wide policy, the CUI Program codifies a baseline of physical safeguarding requirements, identified in [32 CFR 2002](#). While a number of agencies have found that their existing physical safeguarding measures align to the CUI requirements, many have yet to achieve compliance. [CUI Notice 2020-01](#) established a deadline for agencies to implement physical safeguarding for CUI by December 31, 2021.

The status of agency CUI physical safeguarding compliance at the end of FY 2024 is indicated in the chart below, based on self-reporting, including projected dates for implementation as provided by agencies.

Agency	Physical Safeguarding
Ability One Commission	3/15/2025
Administrative Conference of the U.S.	Complete
Advisory Council on Historic Preservation	10/31/2026

Barry Goldwater Scholarship and Excellence in Education Foundation	Complete
Central Intelligence Agency	Complete
Commission of Fine Arts	Not Started
Commission on Civil Rights	Complete
Commodity Futures Trading Commission	Complete
Consumer Financial Protection Bureau	6/1/2026
Consumer Product Safety Commission	4/20/2025
Defense Nuclear Facilities Safety Board	Complete
Denali Commission	12/25/2025
Department of Agriculture	6/30/2025
Department of Commerce	Complete
Department of Defense	Complete
Department of Education	12/31/2024
Department of Energy	Complete
Department of Health and Human Services	6/30/2025
Department of Homeland Security	Complete
Department of Housing and Urban Development	7/1/2025
Department of Interior	9/30/2031
Department of Justice	Complete
Department of Labor	12/31/2025
Department of State	Complete
Department of Transportation	Complete
Department of Treasury	9/30/2025
Department of Veterans Affairs	12/31/2025
Environmental Protection Agency	12/31/2025
Export-Import Bank of the U.S.	Complete
Farm Credit Administration	6/1/2025
Federal Communications Commission	5/31/2025
Federal Election Commission	Complete
Federal Energy Regulatory Commission	Complete
Federal Housing Finance Agency	Complete
Federal Labor Relations Authority	Complete
Federal Maritime Commission	Complete
Federal Mediation and Conciliation Service	Complete
Federal Mine Safety and Health Review Commission	9/30/2025
Federal Retirement Thrift Investment Board	Complete
Federal Trade Commission	Complete
General Services Administration	Complete
Institute of Museum and Library Services	12/30/2025
Inter-American Foundation	Complete
International Development Finance Corporation	Complete
James Madison Memorial Fellowship Foundation	3/1/2025
Marine Mammal Commission	12/31/2025

Merit Systems Protection Board	10/1/2025
Millennium Challenge Corporation	Complete
Morris K. Udall and Stewart L. Udall Foundation	9/30/2026
National Aeronautics and Space Administration	Complete
National Archives and Records Administration	Complete
National Capital Planning Commission	Complete
National Council on Disability	3/31/2025
National Credit Union Administration	9/30/2025
National Endowment of the Arts	3/31/2025
National Labor Relations Board	Complete
National Mediation Board	12/31/2025
National Science Foundation	Complete
National Transportation Safety Board	Complete
Nuclear Regulatory Commission	Complete
Nuclear Waste Technical Review Board	Complete
Occupational Safety and Health Review Commission	3/31/2025
Office of Government Ethics	Complete
Office of Personnel Management	9/30/2025
Office of Special Counsel	Did Not Report
Office of the Director of National Intelligence	Complete
Pension Benefit Guaranty Corporation	Complete
Postal Regulatory Commission	9/30/2025
Railroad Retirement Board	Complete
Securities and Exchange Commission	12/30/2025
Selective Service System	Complete
Small Business Administration	7/1/2025
Social Service Administration	Complete
Surface Transportation Board	9/30/2025
Tennessee Valley Authority	12/30/2025
Trade and Development Agency	6/30/2025
U.S. Access Board	12/31/2025
U.S. African Development Foundation	Did Not Report
U.S. Agency for Global Media	Complete
U.S. Agency for International Development	1/31/2025
U.S. Interagency Council on Homelessness	Not Started
U.S. International Trade Commission	Complete

INFORMATION SYSTEMS SAFEGUARDING

Requirements for information systems safeguarding are identified in [32 CFR 2002.14\(g\)](#).

Federal information systems that are used to store, process, or transmit CUI must

comply with the standards identified in [FIPS PUB 199](#) and be configured at no less than the Moderate Confidentiality impact value. The Moderate impact level for confidentiality indicates that if sensitive data were exposed it could lead to significant consequences, but not catastrophic damage. [CUI Notice 2020-01](#) established a deadline of December 31, 2021, for agencies to implement information systems safeguarding for CUI.

The status of agency CUI information system safeguarding compliance as of the end of FY 2024 is indicated in the chart below, based on self-reporting, including projected dates for implementation as provided by agencies.

Agency	Information Systems Safeguarding
Ability One Commission	3/15/2025
Administrative Conference of the U.S.	Complete
Advisory Council on Historic Preservation	10/31/2026
Barry Goldwater Scholarship and Excellence in Education Foundation	Complete
Central Intelligence Agency	12/31/2027
Commission of Fine Arts	Not Started
Commission on Civil Rights	11/3/2026
Commodity Futures Trading Commission	Complete
Consumer Financial Protection Bureau	9/1/2026
Consumer Product Safety Commission	Complete
Defense Nuclear Facilities Safety Board	Complete
Denali Commission	12/31/2025
Department of Agriculture	7/1/2025
Department of Commerce	Complete
Department of Defense (DoD)	Complete
Department of Education	12/31/2024
Department of Energy	1/2/2027
Department of Health and Human Services (HHS)	12/31/2026
Department of Homeland Security (DHS)	TBD
Department of Housing and Urban Development	7/1/2025
Department of Interior	Complete
Department of Justice	Complete
Department of Labor	12/31/2025
Department of State	Complete

Department of Transportation	9/30/2025
Department of Treasury	9/30/2025
Department of Veterans Affairs (VA)	12/31/2025
Environmental Protection Agency	12/31/2026
Export-Import Bank of the U.S.	Complete
Farm Credit Administration	6/1/2025
Federal Communications Commission	9/30/2026
Federal Election Commission	9/30/2027
Federal Energy Regulatory Commission	Complete
Federal Housing Finance Agency	Complete
Federal Labor Relations Authority	Complete
Federal Maritime Commission	Complete
Federal Mediation and Conciliation Service	Complete
Federal Mine Safety and Health Review Commission	9/30/2025
Federal Retirement Thrift Investment Board	Complete
Federal Trade Commission	Complete
General Services Administration (GSA)	12/31/2025
Institute of Museum and Library Services	12/30/2025
Inter-American Foundation	Complete
International Development Finance Corporation	3/31/2025
James Madison Memorial Fellowship Foundation	3/1/2025
Marine Mammal Commission	Complete
Merit Systems Protection Board	10/1/2025
Millennium Challenge Corporation	12/1/2026
Morris K. Udall and Stewart L. Udall Foundation	9/30/2026
National Aeronautics and Space Administration (NASA)	Complete
National Archives and Records Administration (NARA)	1/1/2026
National Capital Planning Commission	Complete
National Council on Disability	Complete
National Credit Union Administration	9/30/2025
National Endowment of the Arts	3/31/2025
National Labor Relations Board	Complete
National Mediation Board	12/31/2025
National Science Foundation	Complete
National Transportation Safety Board (NTSB)	Complete
Nuclear Regulatory Commission (NRC)	Complete
Nuclear Waste Technical Review Board	Complete
Occupational Safety and Health Review Commission	3/31/2025
Office of Government Ethics	Complete
Office of Personnel Management (OPM)	9/30/2025
Office of Special Counsel	Did Not Report
Office of the Director of National Intelligence (ODNI)	12/31/2029
Pension Benefit Guaranty Corporation	Complete
Postal Regulatory Commission	9/30/2025

Railroad Retirement Board	12/31/2025
Securities and Exchange Commission (SEC)	Complete
Selective Service System	12/31/2025
Small Business Administration	6/1/2025
Social Service Administration	Complete
Surface Transportation Board	9/30/2025
Tennessee Valley Authority (TVA)	12/30/2025
Trade and Development Agency	6/30/2025
U.S. Access Board	12/31/2025
U.S. African Development Foundation (USADF)	Did Not Report
U.S. Agency for Global Media	Complete
U.S. Agency for International Development (USAID)	1/31/2025
U.S. Interagency Council on Homelessness	Not Started
U.S. International Trade Commission	Complete



ADMINISTRATION and ENGAGEMENT

ISOO has several roles and responsibilities related to the administration of presidentially and congressionally established entities, pursuant to [E.O. 13526](#), the [Public Interest Declassification Act](#) as amended, [E.O. 12829](#) as amended, [E.O. 13587](#), and [E.O. 13549](#). The following sections provide an overview of those responsibilities, related activities, and accomplishments.

SUPPORT FOR THE INTERAGENCY SECURITY CLASSIFICATION APPEALS PANEL

The ISCAP provides the public and users of the classification system with a forum for further review of classification determinations made at the agency level. Established by

presidential order in 1995, the ISCAP receives its current guidelines from E.O. 13526. ISCAP members include representatives from the Departments of State, Defense, and Justice, the National Archives and Records Administration, the Office of the Director of National Intelligence, and the National Security Advisor. Additionally, the Director of the Central Intelligence Agency may appoint a temporary representative to participate as a voting member in all ISCAP deliberations and associated support activities concerning classified information originated by the Central Intelligence Agency.

ISCAP has four main functions:

- Decide on appeals by people who have filed classification challenges under [section 1.8](#) of E.O. 13526;
- Approve, deny, or amend agency exemptions from automatic declassification, as provided in [section 3.3](#) of E.O. 13526;
- Decide on appeals by people or entities who have filed requests for mandatory declassification under [section 3.5](#) of E.O. 13526; and
- Inform senior agency officials and the public, as appropriate, of final ISCAP decisions on appeals under sections [1.8](#) and [3.5](#) of E.O. 13526.

ISOO RESPONSIBILITIES

In accordance with [E.O. 13526](#), the Director of ISOO serves as the executive secretary of ISCAP. ISOO staff also provides programmatic and administrative support. This includes assessing the validity of incoming appeals, corresponding with appellants and agencies, preparing appeals for panel discussion, hosting monthly meetings, preparing ballots for decisions, providing appellants and agencies with decisions, and releasing declassified materials.

MANDATORY DECLASSIFICATION REVIEW APPEALS

[E.O. 13526](#) permits the appeal of agency decisions that were made in response to MDR requests. After an agency's denial of an MDR request, the requestor can file an administrative appeal with the agency, which, if denied, can be followed by an appeal to the ISCAP. The ISCAP is the highest appellate body for MDR decision. ISOO processes appeals as they are received to determine whether they are appropriate, in accordance with the [ISCAP bylaws](#), to bring before the ISCAP for adjudication.

The ISCAP rendered decisions for 14 MDR appeals in FY 2024, which is comparable to that of previous years. The ISCAP administratively closed 44 appeals either because they did not meet the requirements for acceptance or because the appellant had withdrawn the appeal. The ISCAP received 34 new appeals in FY 2024, with approximately 1,200 appeals pending, awaiting ISCAP review.

Among the appeals adjudicated by the ISCAP in FY 2024 was [appeal 2014-030](#), a series of documents from the John F. Kennedy Presidential Library regarding U.S. involvement in Laos in 1961 that had been previously classified in full and are now declassified in their entirety.

Also adjudicated in FY 2024 was [appeal 2015-002](#), consisting of 18 documents from the Defense Intelligence Agency providing a view of military intelligence regarding Iraq during the 1991 Gulf War.

The 14 appeals decided upon in FY 2024 included 33 documents with a total of 436 pages reviewed. Twenty of these documents (140 pages) were declassified in full, 6 documents (258 pages) were declassified in part, and 7 documents (38 pages) were affirmed. These, and other records declassified in full or in part, are available via the ISCAP website housed at [NARA.gov](#).

CHALLENGES TO CLASSIFICATION

The ISCAP received and adjudicated one classification challenge appeal submitted by an authorized holder of classified information at the National Security Agency (NSA). The ISCAP voted to affirm the classification decision of the NSA in that appeal but specified granular portion-marking requirements that NSA must follow in the marking of the information that was subject of the classification challenge.

REVIEW OF DECLASSIFICATION GUIDANCE

Additionally, the ISCAP reviewed and approved an updated declassification guide submitted by the Nuclear Regulatory Commission and a file series exemption modification submitted by the Federal Bureau of Investigation.

SUPPORT FOR THE PUBLIC INTEREST DECLASSIFICATION BOARD

The PIDB was established by Congress in 2000, via the [Public Interest Declassification Act](#) to serve in an advisory role to the executive branch, with the official mandate of promoting the fullest possible public access to a thorough, accurate, and reliable documentary record of significant U.S. national security decisions and activities.

The PIDB advises on the identification, collection, and declassification of records of extraordinary public interest, including recommendations for the President on the declassification of specific records as directed by congressional request. The PIDB also advises the President and other executive branch officials on policies deriving from the issuance of Executive Orders by the President regarding the classification and declassification of national security information.

As specified in section 703(c) of the Public Interest Declassification Act, the PIDB is

composed of nine members: five presidential appointees and four congressional appointees (Speaker of the House, House Minority Leader, Senate Majority Leader, and Senate Minority Leader).

ISOO RESPONSIBILITIES

The Director of ISOO serves as the executive secretary of the PIDB in accordance with the Public Interest Declassification Act of 2000, as amended. The ISOO staff provides the PIDB with programmatic and administrative support needed to execute board activities and reporting.

REPORTS AND PUBLICATIONS

The PIDB issues an annual report to Congress based on their activities and recommendations during each calendar year. Included here are highlights from PIDB activities during FY 2024 to illustrate ISOO's support for the Board. The PIDB's full report for calendar year 2024, as well as the Board's previous annual reports to Congress, are [available via the PIDB's website](#) housed at NARA.gov.

PIDB MEETINGS AND CONFERENCES

On June 24, 2024, the PIDB held a public meeting at the National Archives in Washington, DC, featuring presentations on projects for processing Freedom of Information Act (FOIA) requests at the Departments of State and Defense. Representatives from the Department of State (State) outlined the challenges with the large volume of diplomatic cables eligible for declassification review that render human review unsustainable. In 2022, State piloted their implementation of Artificial Intelligence (AI) augmented cables declassification review, followed by their first public release of records reviewed via this process in late 2023.

As of June 2024, 450,000 cables had been reviewed in this process. Building on the success of the first pilot, State launched a second pilot for FOIA review, the 360 FOIA Matching Tool, which is currently in the testing and implementation phase. The Department of Defense (DoD) presentation focused on addressing the necessity of modernizing the department's classified information management declassification program. Representatives from the Applied Research Laboratory for Intelligence and Security provided an overview of the system engineering model for automatic declassification review.

The DoD is also engaging with other federal agencies, including the Department of State, the Department of Energy, and the National Geospatial-Intelligence Agency, on its projects. The speakers and board members stressed the need for high-level government attention, and a coordinated approach, to projects like these, which seek to use technology to modernize classification. The event was live streamed, [and an online recording is available](#).

PIDB members Carter Burwell and Carmen Medina participated in a conference, "The Dark State? Government Secrecy and American Democracy," on April 19, 2024. The conference was presented by the Arnold A. Saltzman Institute of War and Peace Studies and the Institute of Global Politics. Conference presentations focused on the state of secrecy in the American government, the role of Artificial Intelligence in declassification, and classification as well as declassification reform.

ADMINISTRATIVE CHANGES

The National Defense Authorization Act for Fiscal Year 2024 amended the Public Interest Declassification Board Act to specify that a member whose term has expired may continue to serve until a successor is appointed and sworn in, for up to one year

after the date of term expiration. The amended Act also specifies that the PIDB may, subject to the availability of funds, hire not more than twelve staff members.

SUPPORT FOR THE NATIONAL INDUSTRIAL SECURITY PROGRAM

The NISP was established in [E.O. 12829](#), "National Industrial Security Program," on January 6th, 1993, to safeguard federal government classified information that is released to contractors, licensees, and grantees of the United States government. When arrangements with these entities require access to classified information, this information must be safeguarded in a manner equivalent to its protection within the executive branch of government.

To advance national security, our industrial security program must also promote the economic and technological interests of the United States. Redundant, overlapping, or unnecessary requirements impede those interests. As such, the NISP serves as a single, integrated, cohesive industrial security program to protect classified information and to preserve our Nation's economic and technological interests.

Additionally, [E.O. 12829](#) established the NISP Policy Advisory Committee (NISPPAC) as a forum to discuss and facilitate the resolution of program-related policy issues in dispute, and to recommend changes to policies and procedures as reflected in this order, its implementing directives, or the operating manual established under this order.

ISOO RESPONSIBILITIES

Under [E.O. 12829](#), as amended, the Secretary of Defense serves as the Executive Agent responsible for inspecting and monitoring contractors, licensees, and grantees under the program and issues and maintains the National Industrial Security Program Operating

Manual, which prescribes the specific requirements, restrictions, and other safeguards necessary under the program.

The NSC provides overall policy direction for the NISP. The Director of ISOO is responsible for implementation and monitoring of the program, including: the development of directives for the implementation of the E.O.; overseeing actions to ensure compliance with the E.O.; reviewing all agency implementing regulations, internal rules, or guidelines; conducting reviews of the implementation of the NISP; and considering and acting on complaints and suggestions from persons within or outside the government with respect to the administration of the NISP.

E.O. 12829 designates the Director of ISOO as the NISPPAC Chairman. Members of the Committee are representatives of departments and agencies most affected by the NISP, and non-government representatives of contractors, licensees, and grantees involved with classified contracts, licenses, or grants.

NISP ADVANCES IN FY 2024

In FY 2024, there were several areas of growth and improvement across the NISP. Specifically, the Personnel Vetting Questionnaire (PVQ), a form used for background investigations, was approved by the White House Office of Management and Budget. The PVQ streamlined multiple data collections into one electronic form, which will be used in the e-App system where individuals input information to process their personnel background investigation.

Additionally, Trusted Workforce 2.0 policies and guidance were jointly issued to departments, agencies, and investigative service providers, with new standards promulgated for background investigators and security adjudicators that cover vetting

scenarios, investigation upgrades, trust re-establishment, and performance management.

Key processes affecting industry were also streamlined for efficiency in FY 2024. Specifically, the CIA made significant progress in reducing its polygraph backlog and timelines, which resulted in an average processing time for industrial contractors of approximately 60 days. Conditional clearances were also implemented by the Defense Counterintelligence and Security Agency as an efficient alternative to full due process, allowing individuals to be put to work while waiting for final clearance decisions.

NISP POLICY ADVISORY COMMITTEE ACTIVITIES IN FY 2024

The NISPPAC met twice in FY 2024, addressing and discussing issues such as Sensitive Compartmented Information (SCI) indoctrinations, Industry Security Reviews/Scorecards, Facility Security Clearance packages, and leadership prioritization of improving polygraph processes. In addition to NISPPAC meetings, several committee working groups met, addressing issues such as CUI challenges, National Defense Authorization Act section 847 implementation, the entity vetting backlog, and advances made with various technological platforms that are key for industry success.

IMPROVING THE SECURITY OF CLASSIFIED NETWORKS AND THE RESPONSIBLE SHARING AND SAFEGUARDING OF CLASSIFIED INFORMATION

[E.O. 13587](#), “Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information” established the Senior Information Sharing and Safeguarding Steering Committee (Steering Committee), the Classified Information Sharing and Safeguarding Office (CISSO), and the Insider Threat Task Force, all of which support the development and implementation of policies and

minimum standards for sharing classified information on computer networks within and outside the federal government.

As a member of the Steering Committee, CISSO, and Insider Threat Task Force, ISOO has many responsibilities. These include supporting the development of program and budget recommendations to achieve government-wide classified information sharing and safeguarding goals, coordinating the interagency development and implementation of policies and standards for sharing and safeguarding classified information on computer networks, the dissemination of policies, and providing analysis of new and continuing insider threat challenges facing the United States government.

ISOO'S SUPPORT FOR STATE, LOCAL, TRIBAL, AND PRIVATE SECTOR ENTITY CNSI PROGRAMS

The State, Local, Tribal, and Private Sector Policy Advisory Committee (SLTPS-PAC) was established by [E.O. 13549](#), "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities," to discuss program-related issues in dispute to facilitate their resolution and designated the Director of ISOO as its executive secretary. The SLTPS-PAC also recommends changes to policies and procedures to remove impediments to the sharing of information under the program.

ISOO RESPONSIBILITIES

Under [E.O. 13549](#), as amended, the Secretary of Homeland Security serves as the Executive Agent responsible for safeguarding and governing access to classified national security information shared by the federal government with state, local, tribal, and private sector (SLTPS) entities. The Director of ISOO's responsibilities include considering and acting on complaints and suggestions from persons within or outside

the government with respect to the administration of the sharing of classified information with the SLTPS.

This E.O. also designates the Director of ISOO as the SLTPS-PAC Chairman, and the members of the Committee are representatives of departments and agencies most affected by the sharing of classified information with the SLTPS, along with SLTPS-PAC entities.

SLTPS-PAC ACTIVITIES IN FY2024

The SLTPS-PAC met twice in FY 2024, with a primary focus on DHS's security clearance backlog for the SLTPS community. DHS's Office of Intelligence and Analysis created a clearance prioritization and categories list to rank requests, a process to re-validate need to know, and a method to tie verified justifications directly to the Homeland Security Mission. Those efforts resulted in a 60% reduction in backlogged security clearances. Additionally, DHS initiated an administrative review of security clearance holders and identified over 750 personnel for security clearance removal.



NATIONAL ARCHIVES

Information Security Oversight Office
National Archives and Records Administration
700 Pennsylvania Avenue, N.W. Room 100
Washington, D.C. 20408-0001

www.nara.gov/isoo

*Images of the Inlaid Bronze Medallion, Rotunda Lobby
Jeff Reed, 2017-08-09, From the collection of the National Archives*