

INFORMATION SECURITY OVERSIGHT OFFICE

ISOO 2025 ANNUAL REPORT

TO THE PRESIDENT OF THE UNITED STATES

Fiscal Year 2025
Annual Report to the President of the United States

September 30, 2026

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

September 30, 2026

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

Dear Mr. President,

I am pleased to provide the Annual Report of the Information Security Oversight Office for Fiscal Year 2025, prepared for your review, responsive to the requirements of Executive Order 13526, "Classified National Security Information," and Executive Order 13556, "Controlled Unclassified Information."

ISOO serves as the steward of our nation's secrets – an on-field referee for how the American government handles its most sensitive information. We help explain and enforce the rules set out under your authority as Commander in Chief: what requires protection, why, and for how long. In doing so, we strive to ensure that our nation derives the fullest value from the extraordinary breadth of information created, collected, managed, and maintained by our government, while also ensuring that appropriate public access remains a fundamental part of how that value is assessed.

This report, intended to inform and support 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 and also includes sections on additional institutions and activities ISOO leads and manages at your direction, including the Interagency Security Classification Appeals Panel, the National Industrial Security Program, and the Public Interest Declassification Board.

In executing these duties, ISOO often, and rightly, confronts the tension that exists between our government's dual imperatives of secrecy and transparency. There are few today who would argue the fact that our government still keeps far too many secrets for

far too long. The reasons for this hoarding are multifaceted and long-standing, a product of cultural norms and structural challenges that, while widely recognized, have proven exceedingly difficult to resolve, decade after decade.

Your administration has acted decisively to declassify and release information in the public interest. This extraordinary intervention has provided a much-needed pressure-release valve, making good on overdue commitments and moving high-value information more readily into the public sphere. However, the system as a whole remains under tremendous strain. With this strain comes risk – to the national security of the United States, to the essential services that our citizens depend on, and to the trust our people place in government to act responsibly and accountably on their behalf.

These risks are no doubt familiar, but the sudden and staggering pace of advancement in information technology, particularly the commercial application of Super Intelligence, and the attendant transformations underway in our society and the global economy, are reshaping familiar risks more rapidly than their evolving impact can be fully assessed. In the process, they call into sharp relief the need for long-lagging investments to modernize how the American government manages its information.

While the full measure of risk we face remains murky, it is already clear that these same technologies are poised to revolutionize the entire lifecycle of government information. End-to-end automation made possible by integrated, intelligent records management solutions, within and across agencies, will transform how we create, securely share, and prepare for public release the documents, data, multimedia, and machine-driven models that form the future of how our government will operate. This new infrastructure will likewise offer unprecedented opportunities for oversight: analytics, insight, transparency, and accountability, to assess how information is being marshaled and managed to serve an ever-wider array of stakeholders and urgent national interests. This is the foundation that will finally bring true reform to the "last mile," enabling a more regular, fulsome, and timely release of information to the public.

Just as importantly, these tools will enable better use of America's secrets when and while circumstances demand that we still keep them. This ability to prevent the indiscriminate release of information is how our government preserves privacy, how we guard intellectual property, how we help ensure economic prosperity, and, of course, how we continue to protect our national security. It is a power and a premise that we owe to America's founders, who recognized secrecy as a necessary attribute of

sovereignty, vital to the survival of the United States as an independent nation. At the same time, as we reach the 250th anniversary of the American experiment, we should not let it be lost in the periphery of history's sometimes narrow gaze that the primal act of making America was not the secret signature of 56 founders on a piece of parchment, but rather how the people of our nascent nation were enabled and empowered by the swift and sure sharing of this information.

The United States still needs its secrets today as much as it ever has. The challenge currently before us is not deciding between protection and access or finding a "balance" between secrecy and transparency. It is, instead, the obligation to build a government capable of managing each with greater precision, discipline, and speed. Safeguarding and sharing are both critical functions for securing our democracy and both must be tended well by the system that governs our most sensitive information. It is this pillar of our public institutions that ISOO exists to serve. As you will see reflected in the report that follows, the technologies now emerging provide us an opportunity to do this in ways that were previously impossible: to protect what must remain protected, to make better use of the information we hold, and to move what no longer requires protection into the hands of those who can use it to the further benefit of our nation and the world.



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 13

ISOO's Oversight Of The Controlled Unclassified Information Program 14

GUIDANCE and IMPLEMENTATION 16

Guidance Issued by ISOO 16

Federal Acquisition Regulation for CUI 17

DATA COLLECTION and ANALYSIS 18

Implementation of Super Intelligence On Classified Systems 19

Analysis of Department and Agency Expenditures for the CNSI System 20

Original Classification Authority Designations 20

Evaluation of the Declassification-Focused Federal Workforce 21

Mandatory Declassification Review Performance 23

CNSI Related Security Violations 23

CUI Program Implementation at Federal Departments and Agencies 24

ADMINISTRATION and ENGAGEMENT 30

Interagency Security Classification Appeals Panel 30

ISOO Responsibilities 31

Mandatory Declassification Review Appeals 32
Challenges to Classification 33
Review of Declassification Guidance 33
The Public Interest Declassification Board 33
ISOO Responsibilities 34
Reports and Publications 34
PIDB Meetings and Conferences 34
Administrative Changes 35
The National Industrial Security Program 36
ISOO Responsibilities 37
NISP Advances in FY 2025 37
NISP Policy Advisory Committee Activities in FY 2025 38
Improving the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information 39
State, Local, Tribal, and Private Sector Entity CNSI Programs 40
ISOO Responsibilities 40
SLTPS-PAC Activities in FY 2025 41

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 War, 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 (NISPPAC) 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 is the central governance body responsible for overseeing all sensitive information—Classified and Unclassified—created, managed, and maintained by the federal government, serving both the President and the public. This authority extends to information both 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 national defense and foreign relations. This system protects information determined to require safeguards against unauthorized disclosure. Information is classified at one of three

levels, which establish discrete standards for secure management based on the assessed damage to national security resulting from 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 national security.

Governance of CNSI is broadly defined by E.O. 13526, "Classified National Security Information," which outlines 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 to executive branch agencies and oversee compliance. This mandate 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 CNSI program effectiveness and enforce compliance with directives such as E.O. 13526. Pursuant to sections 5.2(b)(2) and (4) of the Order, ISOO examines security education, agency SCGs, document markings, and management practices. ISOO also verifies the proper use of delegated Original Classification Authority. Reported OCA delegations for FY 2025 are detailed in the Data Collection and Analysis section of this report.

ISOO performed six agency on-site inspections and reviewed ten SCGs during FY 2025,

representing an increase over the five inspections conducted and nine guides reviewed in FY 2024. Methodology improvements have resulted in more efficient reviews that yield more actionable data while reducing administrative burdens on agencies. This includes a new hybrid inspection approach—incorporating remote employee interviews and digital reviews of documents, SCGs, and training materials— which has significantly reduced time required on-site. Inspections from FY 2013-23 required an average of four days on-site; in FY 2025, inspections required an average of only one and a half days on-site. This hybrid approach minimizes the interruptions to daily business that are a necessary part of the inspection process, to ensure agencies can continue to perform their vital work for the American people.

ISOO's quantitative scoring methodology, fully implemented in FY 2025, provides agencies with overall compliance scores and granular, item-by-item data. Agencies can now clearly identify areas of excellence or necessary improvement. Core areas include:

- Security Classification Guides – Average FY 2025 Agency Score: **82.5%**
- Security Education and Training – Average FY 2025 Agency Score: **92.1%**
- Security Program Management – Average FY 2025 Agency Score: **89.2%**
- Marking of Classified Documents – Average FY 2025 Agency Score: **89%**

Security Classification Guide Assessments

Federal personnel with delegated OCA create and maintain SCGs under E.O. 13526 section 2.2(a) and 32 CFR Parts 2001.11 and 2001.15. These guides serve as the central repository for classification decisions, ensuring unique agency information is adequately protected. SCGs must clearly explain classification rationales to prevent

over-classification or unnecessary barriers to information sharing. ISOO's periodic reviews of these guides are vital to assessing CNSI program health.

In FY 2025, as a component of its agency inspections, ISOO evaluated ten SCGs from the Environmental Protection Agency (EPA), Defense Advanced Research Projects Agency (DARPA), Department of Health and Human Services (HHS), Department of Energy (DoE), and Department of State (DoS). The US Department of Transportation (USDOT) did not provide an SCG for review. The average score for this section was 82.5%. DARPA achieved a perfect score of 100%, while the DoS, DoE, and HHS all exceeded 90%.

Notably, the USDOT lacked a security classification guide despite reporting eight individuals with OCA and active derivative classification activity, a potential violation of 32 CFR 2001.15. ISOO assigned USDOT a score of 47% in this segment as they possessed some documentation but no formalized guide. The EPA has two individuals with OCA and conducted derivative classification but lacks a comprehensive SCG, instead developing limited-scope SCGs on an ad hoc basis. This practice deviates from community standards, as it can lead to contradictory classification decisions and lacks necessary socialization among personnel. ISOO assigned EPA a score of 70% in this segment.

In FY 2025, DoS and HHS modernized their SCGs to align with the current classification environment and technology. ISOO assisted by reviewing drafts and providing feedback for better compliance. Both draft SCGs were exemplary; HHS scored 95% and DoS scored 92.5%. The three most significant issues observed across all agency SCGs were:

- Three guides among three agencies failed to map classification levels to specific information elements per 32 CFR Part 2001.15(b)(6);
- One guide did not include the required declassification dates or events per 32 CFR Part 2001.15(b)(9); and
- Three guides across three agencies lacked specific classification reasoning per 32 CFR Part 2001.15(b)(8).

Security Education and Training

Effective security training is critical for the proper handling of CNSI, the prevention of security incidents, and the protection of national security. ISOO evaluates these materials for compliance with 32 CFR Parts 2001.70 and 2001.71. In FY 2025, ISOO inspected training programs at USDOT, EPA, DARPA, HHS, DoE, and DoS. Most agencies performed well, with an average score of 92.1%. The lowest overall score was HHS at 82.5%, while EPA and DoE each earned scored 97.5%, which was the highest score.

A primary trend observed amongst the agencies evaluated by ISOO in FY2025, was the consolidation of disparate topics into a single training module to reduce employee burden. While often satisfactory, this occasionally resulted in missing key requirements. The main deficiencies that were observed were the failure to explain penalties for mishandling CNSI or conducting espionage, and the omission of foreign government information protocols. These elements are covered in the "Annual Refresher Training" segment, which was the lowest-performing segment overall with an average score of 83.3%.

Initial employee training

ISOO inspects initial employee training per E.O. 13526 section 4.1(b) and 32 CFR

2001.70(b) and 2001.71(b). During FY 2025 inspections, most agencies were compliant, averaging 89.6%. The primary issue remains the omission of penalties for mishandling CNSI within combined training modules.

Original Classification Authority Training

Training for employees with OCA is mandated by 32 CFR Parts 2001.11(a) and 2001.70(c) upon appointment and at least annually thereafter. During inspections, all six agencies demonstrated that initial OCA training had occurred. The average score for this training was 87.5%. Two agencies did not cover SCG development or maintenance—a key component of the OCA role—and one failed to cover classification elements, although this was addressed in their mandated Annual Refresher Training.

Derivative Classification Training

Personnel holding a security clearance generally have the authority to derivatively classify information—the ability to summarize, reproduce, or use existing classified information as a source for communications or analysis. All six agencies were found to be providing derivative training that complies with the requirements in 32 CFR 2001.71(d), with an average score of 97.9%. The DoS training received an 87.5% as it did not adequately cover classification prohibitions, limitations, or sanctions.

Annual Refresher Training

All employees handling classified information must receive annual refresher training per 32 CFR 2001.71(f). This training must reinforce existing policies, cover foreign government information, detail threats from foreign intelligence entities, and emphasize penalties for espionage. Three of the six agencies reviewed did not adequately cover these threats. ISOO noted that USDOT lacked appropriate enforcement mechanisms for compliance, and HHS only mandates refresher training

for individuals with access to Sensitive Compartmented Information (SCI). This section was the worst performing, with an average score of 83.3%.

Specialized Security Training

Under 32 CFR 2001.71(e), agencies must provide specialized training to personnel with specific responsibilities, such as security managers and couriers, within six months of assuming those duties. Among smaller agencies, this training is often informal or "on the job" at the unit level. However, ISOO found all six inspected agencies had training meeting the requirements of this category.

Security Program Management

Successful CNSI program implementation requires effective management from an agency's security elements. ISOO evaluates effectiveness based on preparedness, staffing, internal training, leadership support, and compliance mechanisms. ISOO found that while some agencies utilize in-house programs, others rely on external organizations like the Center for Development of Security Excellence.

Larger organizations with more robust programs are typically better managed. In FY 2025, USDOT and EPA performed lower than average (both earning 77.5% compared to the 89.2% average). ISOO assesses that this was primarily due to significant staffing shortages. These issues existed prior to current federal-wide efficiency initiatives and may have been exacerbated by recent retirements. For both organizations, a single small team manages CNSI, Industrial Security, Physical Security, and CUI elements.

Of the inspected organizations, all except DARPA and HHS reported significant staffing shortages. In response, DoE and DoS have deployed Super Intelligence and Large Language Models to support classification and declassification programs. While promising, these initiatives require adequate funding, specialized training, and,

potentially, new personnel in order to realize their full potential.

ISOO also observed gaps in training enforcement and off-boarding. At USDOT, security managers cannot remove access for personnel who are non-compliant with training.

Marking of Classified Documents

ISOO examines classified documents to ensure compliance with E.O. 13526 section 1.6 and 32 CFR 2001.20-26. ISOO aims to review approximately 1% of an agency's derivatively classified documents. This review serves as a key indicator of training effectiveness and an agency's overall security posture. Documents are assessed for markings, classification levels, and correct Classification Authority Blocks (CABs).

ISOO recommends the use of Classification Marking Tools (CMTs) for emails. CMTs help users apply accurate banners and CABs and when employed properly are effective in reducing over-classification and preventing data spillage. Agencies received an average score of 90% in this category, with USDOT earning 100%. With an average score of just 68.8%, CABs were the most significant challenge for the inspected agencies. HHS, DoE, and DARPA all struggled in this area. Other common issues include the omission of CUI warning statements on commingled documents, citing "multiple sources" without an attached source list, and failing to show appropriate exemption codes.

Improvements and The Way Forward

ISOO is refining its inspection framework for FY 2026 by integrating new programmatic areas of review, specifically Information Technology and CUI. This expansion aims to bolster the oversight program, ensuring agencies meet legal requirements for the safeguarding, marking, training, and dissemination of information. By developing specialized rubrics and evaluation criteria, staff are in the process of transitioning from

a primary focus on CNSI to a more holistic assessment model for information security that will include evaluation of CUI and declassification programs. These improvements are designed to offer reviewed agencies comprehensive reports and actionable data on the full range of their responsibilities under presidential direction, law, regulation, and government-wide policy.

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 2025, ISOO received inquiries from eleven different non-governmental organizations reporting the identification of potentially classified material found outside of government control. In seven 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 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.

32 CFR 2002 implemented the CUI program requirements for safeguarding, disseminating, marking, decontrolling, and disposing of CUI and 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. Agencies report annually to ISOO on the status of their implementation of the program in the form of annual compliance report. This reporting includes questions on compliance with safeguarding, disseminating, marking, decontrolling, disposition, and waivers of requirements for CUI program implementation. As part of this annual reporting cycle moving forward, ISOO will request, review, and process any agency waivers to ensure their compliance with E.O. 13556 and 32 CFR 2002. In FY 2026, ISOO plans to formally incorporate CUI oversight elements into its on-site inspection program.

To facilitate the legally compliant and effective implementation of the CNSI and CUI programs across various agencies, ISOO provides oversight through the consistent development and issuance of policy and guidance. This process involves engagement in interagency collaborations aimed at improving program implementation.

GUIDANCE and IMPLEMENTATION

To facilitate the legally compliant and effective implementation of the CNSI and CUI programs across various agencies, ISOO provides oversight through the consistent development and issuance of policy and guidance. This process involves engagement in interagency collaborations aimed at improving program implementation.

Guidance Issued by ISOO

Pursuant to ISOO's authorities under E.O. 13526, ISOO issued ISOO Notice 2025-01, "Incorporating Automatic Declassification Exemptions into Security Classification Guidance," on September 8, 2025. This notice provides guidance on the proper use and incorporation of automatic declassification exemptions that have been approved by the ISCAP into agency SCGs. ISOO Notices are binding directives on departments and

agencies, 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.

Federal Acquisition Regulation for CUI

In FY 2025, the Federal Acquisition Regulation's CUI rule was published as a proposed rule for public comment on January 14, 2025. This regulation provides specific requirements for contractor and subcontractor handling and safeguarding of CUI, including standardized cybersecurity requirements. At the time of publication of this report, the regulation has still not been issued as a final rule.

DATA COLLECTION and ANALYSIS

Pursuant to E.O.s 13526 and 13556, as well as 32 CFR Parts 2001.90(b) and 2002.8(c)(6), agencies report data regarding their CNSI and CUI programs to ISOO. This information, gathered through an annual data call, provides essential statistics and analysis. These insights enable our oversight team to identify and prioritize specific areas of focus when conducting agency inspections. For FY 2025, ISOO implemented the first major update to its annual Security Compliance Survey in five years. We refined existing questions for greater specificity and introduced new data categories to better reflect the modern operating environment. Notably, the revised survey now captures data on how agencies leverage emerging technologies, such as Super Intelligence, to assist with classification and declassification processes.

Implementation of Super Intelligence On Classified Systems

In FY 2025, six agencies—the Departments of Energy, State, Treasury, and War, along with the Office of the Director of National Intelligence (ODNI) and the Central Intelligence Agency (CIA)—reported implementing Super Intelligence or Large Language Models (LLMs) to enhance classification and declassification workflows. These tools collectively improve the speed, accuracy, and efficiency of these processes while significantly reducing the administrative burden on personnel.

The following agency-specific implementations highlight the diverse utility of these technologies:

- **The Department of State** successfully utilizes machine-assisted review for automatic declassification and to assist staff in the accurate classification of diplomatic cables and correspondence.
- **The ODNI** leverages Super Intelligence to cross-check documentation against SCGs, ensuring consistent and appropriate classification.
- **The CIA** employs specialized tools to identify duplicative information during document reviews and to verify classification accuracy.
- **The Department of Energy** launched the Advanced Computer Tools for Identifying Classified Information (ACTICI) program in FY 2025, with full implementation expected by early FY 2026. This system assists in the automatic identification of classified subjects based on SCGs and facilitates proper marking.

ISOO maintains that the successful implementation of these tools represents a vital and well-executed leap toward modernization. These technologies are essential for

addressing staffing resource gaps and the backlog of MDR requests, which currently exceeds 11,600 unresolved for over one year across the community. Widespread adoption of these tools has the potential to significantly improve turnaround times, consistency of review standards, and overall system integrity.

Analysis of Department and Agency Expenditures for the CNSI System

Under E.O. 13526 section 5.4(d)(8) and 32 CFR 2001.90(c), ISOO collects annual cost-related data for the CNSI system. Historically, this data has fluctuated significantly, complicating the effort to draw reliable conclusions at either the agency or system level. A primary example of this instability is evident in the reported costs for CNSI security clearance investigations and reinvestigations.

The reported expenditures in this category have shifted dramatically over the last five fiscal years. In FY 2021, agencies reported a total of $1.5 billion, which then plummeted to approximately $714 million in FY 2022—a reduction of over 50%. This downward trend continued into FY 2023, with reported totals dropping another 50% to approximately $300 million. However, FY 2024 saw a sharp reversal, as reported costs rose to just over $983 million, representing a more than 200% increase over the previous year. Most recently, in FY 2025, these expenditures exceeded $1.19 billion.

Original Classification Authority Designations

Original Classification Authority, or OCA, refers to the initial determination that information requires protection based on the reasonable expectation of damage to U.S. national security if disclosed without authorization, as defined in E.O. 13526. This authority is strictly limited to the President, the Vice President, and officials specifically designated or delegated under the procedures set forth in the Order. Agencies

document these original classification decisions and their supporting rationales in SCGs to ensure accurate and consistent classification across the federal government.

Agencies managing classified information delegate OCA to specific individuals who then bear organizational responsibility for maintaining SCGs and performing other specialized classification and declassification functions. To remain consistent with E.O. 13526, these delegations must be limited to the minimum number required to effectively administer a CNSI program. Agency heads must also ensure that subordinate officials have a demonstrable and continuing need for this authority. Per E.O. 13526, agencies are required to report all OCA delegations to the Director of ISOO.

While the number of OCA delegations has remained relatively stable over time, FY 2025 saw a 9.5% decrease, dropping from 1,661 to 1,504. In FY 2025, agencies reported:

- 683 Top Secret-level OCAs
- 817 Secret-level OCAs
- 4 Confidential-level OCAs

	# of OCAs				
Classification Level	2021	2022	2023	2024	2025
Confidential	3	3	3	4	4
Secret	946	935	979	963	817
Top Secret	702	700	696	694	683
Total	1651	1638	1678	1661	1504

Evaluation of the Declassification-Focused Federal Workforce

ISOO collects annual data from agencies with declassification programs to determine

the number of Full-Time Equivalent (FTE) employees whose primary duty is declassification. For FY 2025, agencies reported a total of 1,113 declassification-focused FTEs, representing a nearly 20% decrease from the 1,384 reported in FY 2024, and a 40% decrease from 1,883 in FY 2021. ISOO tracks these personnel across twelve discrete functional areas, as detailed in the table below. Because FTE calculations are based on total hours worked rather than individual headcounts, agencies often report fractional figures; consequently, the following data has been rounded to the nearest whole number.

	# of Full-Time Employees				
Declassification Activity	2021	2022	2023	2024	2025
Automatic Declassification	373	389	288	390	234
Systematic Declassification	113	131	47	45	138
Ad Hoc Declassification	87	96	52	48	53
Prepublication Review	112	177	65	58	94
Court-Related Declassification	116	105	67	72	66
NATO / International Use	91	59	35	16	33
Freedom of Information Requests	516	580	476	539	200
Mandatory Declassification Review	144	159	63	97	135
ISCAP Declassifications	68	49	39	23	35
Declassification by Law or Regulation	98	147	96	38	51
Congressional-Related Action	85	58	31	19	33
Foreign Relations of the United States	80	85	38	39	41
Total	1883	2035	1297	1384	1113

ISOO also captured data regarding the human resources devoted to agency CNSI self-inspection programs. Across the federal government, the total number of FTEs dedicated to this oversight function reached 682, which is a 5% increase over the 649 reported in 2024.

Mandatory Declassification Review Performance

ISOO tracks the status of requests for MDR across the federal government to provide visibility into the health of agency declassification programs. While individual agencies are responsible for the actual processing and review of these records, ISOO monitors the number of requests that remain unresolved for more than one year as a primary indicator of system-wide backlogs.

Data from the last five fiscal years highlights a period of significant inventory pressure followed by recent stabilization. The number of unresolved requests peaked during FY 2022 and FY 2023, with request backlogs reaching 22,861 and 22,159, respectively. However, focused agency processing efforts in FY 2024 resulted in a major breakthrough, reducing the backlog by nearly 50% to 11,552. This improved performance was successfully maintained through FY 2025, which ended with 11,627 unresolved requests. By tracking these outcomes, ISOO ensures that policymakers can identify where resource constraints exist and where agencies are successfully prioritizing the public's right to know.

CNSI Related Security Violations

ISOO monitors the integrity of the CNSI system by tracking agency-reported security violations and unauthorized disclosures. FY 2025 marked a significant turning point in this oversight capability, as the annual survey transitioned from a binary "Yes/No" reporting model to capturing specific incident counts. This shift revealed a more detailed picture of the security landscape: 13 agencies identified a total of 6,314 individual security violations.

Agency	# of Reported Violations
Department of Defense	5850
Department of Energy	207
Office of the Director of National Intelligence	122
Department of Homeland Security	104
U.S. Department of Justice	13
NASA	8
US Department of Transportation	3
Peace Corps	2
Environmental Protection Agency	1
Office of Security, U.S. Department of Commerce	1
National Archives and Records Administration	1
U.S. Department of Agriculture	1
Department of the Treasury	1
Total	6314

CUI Program Implementation at Federal Departments and Agencies

The CUI program standardizes how the executive branch handles unclassified information that requires safeguarding or dissemination controls. Prior to the establishment of the CUI program, agencies employed ad hoc, localized 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, including 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.

Each year, as part of its annual compliance survey, ISOO requests information from federal agencies to assess the status of their CUI program implementation. In FY 2025

ISOO revised and streamlined its CUI queries, including specific questions on the implementation of Super Intelligence as a way to gauge the impact such modernization efforts are having on the CUI program. ISOO focused its data gathering on the implementation efforts of 15 cabinet-level departments and 60 other independent agencies, with plans to expand this CUI-related data collection in FY 2026.

The key benchmark ISOO uses to assess agency compliance is whether the agency has a CUI policy to implement the requirements of E.O. 13556 and 32 CFR 2002. Across the executive branch, of the agencies polled in FY 2025, 63% of agencies indicated they had a CUI policy, whereas 37% did not.

For the agencies which did not have CUI policy, among the reasons given for non-compliance were limited financial and personnel resources to commit to the CUI program; lack of leadership that has the (appropriate SES-level) authority to implement a final CUI policy; and having a CUI policy still in the draft phase. Some agencies also referenced waivers of certain CUI requirements as a reason for non-compliance. All such waivers must meet the requirements for one of the three types of waivers authorized in 32 CFR 2002.38: limited CUI marking waivers within the agency; limited legacy material marking waivers within the agency; or exigent circumstances waivers. For all waivers, the requirements that agencies must adhere to are listed in 32 CFR 2002.38(d) and (e). As part of the annual CUI reporting cycle, ISOO will ensure that CUI Senior Agency Officials (SAOs) are meeting their obligations in accordance with these sections.

The following chart indicates which agencies have CUI policy and those that are currently non-compliant with meeting this CUI program requirement.

Agency	Policy
Ability One Commission	Complete
Administrative Conference of the U.S.	Complete
Advisory Council on Historic Preservation	Complete
Barry Goldwater Scholarship and Excellence in Education Foundation	Complete
Central Intelligence Agency	Not Complete
Commission of Fine Arts	Did Not Report
Commission on Civil Rights	Not Complete
Commodity Futures Trading Commission	Not Complete
Consumer Financial Protection Bureau	Not Complete
Consumer Product Safety Commission	Not Complete
Defense Nuclear Facilities Safety Board	Complete
Denali Commission	Not Complete
Department of Agriculture	Complete
Department of Commerce	Complete
Department of Education	Complete
Department of Energy	Complete
Department of Health and Human Services (HHS)	Not Complete
Department of Homeland Security (DHS)	Complete
Department of Housing and Urban Development	Complete
Department of Interior	Complete

Department of Justice	Complete
Department of Labor	Complete
Department of State	Not Complete
Department of Transportation	Complete
Department of Treasury	Complete
Department of Veterans Affairs (VA)	Complete
Department of War (DoW)	Complete
Environmental Protection Agency	Complete
Export-Import Bank of the U.S.	Complete
Farm Credit Administration	Complete
Federal Communications Commission	Not Complete
Federal Election Commission	Not 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	Did Not Report
Federal Mine Safety and Health Review Commission	Not Complete
Federal Retirement Thrift Investment Board	Complete
Federal Trade Commission	Complete
General Services Administration (GSA)	Complete
Institute of Museum and Library Services	Complete

Inter-American Foundation	Did Not Report
International Development Finance Corporation	Complete
James Madison Memorial Fellowship Foundation	Not Complete
Marine Mammal Commission	Not Complete
Merit Systems Protection Board	Not Complete
Millennium Challenge Corporation	Complete
Morris K. Udall and Stewart L. Udall Foundation	Not Complete
National Aeronautics and Space Administration (NASA)	Complete
National Archives and Records Administration (NARA)	Not Complete
National Capital Planning Commission	Complete
National Council on Disability	Not Complete
National Credit Union Administration	Complete
National Endowment of the Arts	Complete
National Labor Relations Board	Complete
National Mediation Board	Not Complete
National Science Foundation	Complete
National Transportation Safety Board (NTSB)	Complete
Nuclear Regulatory Commission (NRC)	Complete
Nuclear Waste Technical Review Board	Not Complete
Occupational Safety and Health Review Commission	Not Complete
Office of Government Ethics	Complete
Office of Personnel Management (OPM)	Not Complete

Office of Special Counsel	
Office of the Director of National Intelligence (ODNI)	
Pension Benefit Guaranty Corporation	
Postal Regulatory Commission	
Railroad Retirement Board	
Securities and Exchange Commission (SEC)	
Selective Service System	
Small Business Administration	
Social Service Administration	
Surface Transportation Board	
Tennessee Valley Authority (TVA)	
Trade and Development Agency	
U.S. Access Board	
U.S. African Development Foundation (USADF)	
U.S. Agency for Global Media	
U.S. Interagency Council on Homelessness	
U.S. International Trade Commission	

ADMINISTRATION and ENGAGEMENT

In accordance with E.O. 13526, the Public Interest Declassification Act, E.O. 12829, as amended, E.O. 13587, and E.O. 13549, ISOO maintains various duties and functions related to the administration of presidentially and congressionally established entities. Summaries of these duties, as well as associated initiatives and successes, are detailed in the subsequent sections.

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, War, 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

The Director of ISOO acts as the executive secretary for ISCAP as established by E.O. 13526. Administrative and programmatic assistance is provided by ISOO staff, who are responsible for evaluating appeal validity and maintaining correspondence with agencies and appellants. Their duties further encompass organizing monthly meetings, preparing appeals for panel review, managing decision ballots, notifying relevant parties of outcomes, and overseeing the release of declassified information.

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 8 MDR appeals in FY 2025, which is fewer than in previous years. This was, in part, a function of the transition of the ISCAP Chair, who is responsible for approving ballots that produce final decisions. A ballot was approved at the end of FY 2025, for review by the Chair with the release decisions rendered early in FY 2026. Additionally, the ISCAP administratively closed 7 appeals either because they did not meet the requirements for acceptance or because the appellant had withdrawn the appeal. The ISCAP received 45 new appeals in FY 2025, with approximately 1,250 appeals pending, awaiting ISCAP review.

Among the appeals adjudicated by the ISCAP in FY 2025 was appeal 2016-036, a 1966 National Intelligence Estimate from the CIA concerning West German capabilities and intentions to produce and deploy nuclear weapons.

Also adjudicated in FY 2025 was appeal 2020-015, which concerns a 1980 Defense Intelligence Agency memorandum to the Secretary of War regarding false missile alerts.

These, and other records declassified in full or in part, are available via the ISCAP website housed at NARA.gov.

Challenges to Classification

Authorized holders of classified information who, in good faith, believe that the classification status is improper are encouraged to challenge the classification status of the information. Agencies must establish procedures allowing for this process. Holders are encouraged to file an informal challenge before a formal challenge. If the challenge is denied or there is no response within a specific timeframe, authorized holders can appeal to the ISCAP. The ISCAP received no challenges to classification in FY 2025.

Review of Declassification Guidance

Agencies formalize its declassification guidance in ISCAP-approved declassification guides. These guides set the parameters by which reviewers of information that is up for declassification can exempt the information for an additional 25 years. These guides differ from SCGs in that they are used during the review of information subject to automatic declassification at 25 years. At least one year before information is subject to automatic declassification, agencies must inform the ISCAP of any proposed exemptions.

The ISCAP reviewed and approved updated declassification guides submitted by the Joint Staff, the Air Force, the National Security Agency, and the Department of the Navy in FY 2025.

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 2025 to illustrate ISOO's support. The PIDB's full report for calendar year 2025, as well as previous annual reports to Congress, are available via the PIDB's website housed at NARA.gov.

PIDB Meetings and Conferences

The PIDB undertook extensive planning throughout 2025 for a public meeting to be held in the U.S. Capitol. Although originally planned for October 2025, the meeting was

ultimately rescheduled for January 14, 2026, due to a federal government shutdown. The event was designed to highlight the need for greater transparency on 9/11-related records approaching their 25-year automatic declassification review deadline This looming milestone has drawn increasing public attention and underscores the importance of ensuring that agencies are prepared to meet their declassification obligations. The PIDB recommends two historically significant sets of records for priority declassification:

- The 9/11 Commission's President's Daily Brief Summary, a 7,000-word synthesis of intelligence reporting on al-Qaeda, Osama bin Laden, and Afghanistan in the three years preceding the attacks.
- The 9/11 Commission's collection of seventeen interview transcripts with the President and Vice President, senior national security officials, and subject-matter experts, created to support the Commission's statutory mandate to investigate the attacks and recommend corrective measures.

The PIDB has consistently championed the review and release of these records, emphasizing that their continued classification more than two decades after the attacks raises serious concerns about transparency, accountability, and public trust. At the same time, the PIDB views the challenges in achieving public accessibility for these records as emblematic of broader systemic deficiencies—underscoring the need for modernization and adequate resourcing in the declassification process.

Administrative Changes

The PIDB onboarded four new members—Mark Angelson (Chair), John W. McCarthy, Ryan Montoya, and Valdez Butler Demings—and reappointed Carter Burwell to a

second term, ensuring both renewed expertise and continuity in the PIDB's statutory oversight and advisory responsibilities.

Additionally, the PIDB updated its bylaws, effective July 16, 2025, in accordance with statute. The bylaws are publicly available on the PIDB's website housed at NARA.gov.

The National Industrial Security Program

The National Industrial Security Program (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

The National Security Council provides overall policy direction for the NISP, with the Director of ISOO, under E.O. 12829, as amended, 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. The Secretary of War 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.

NISP Advances in FY 2025

In FY 2025, there were several areas of growth and improvement across the NISP driven by the Defense Counterintelligence and Security Agency's (DCSA) 2025-2030 Strategic Plan. DCSA implements directives of the Department of War (DoW). The focus has shifted from a catch-up mode, to a proactive, data-driven security model. Specifically, the Personnel Vetting Questionnaire, a form used in the e-App system for background investigations, was rolled out for Industry in 2025 to test and refine the user experience,

streamlining multiple data collections into one electronic form.

Additionally, Trusted Workforce 2.0 was expanded to incorporate updated continuous vetting policies and guidance for Industry, including new standards promulgated for background investigators and security adjudicators that cover vetting scenarios, investigation upgrades, trust re-establishment, and performance management.

FY 2025 marked a pivot toward the next generation of security systems. DCSA started reengineering workflows to allow better data flow between entities in the federal government. While the National Background Investigation Services, often referred to as the NBIS platform, remains a work in progress, DoW has committed to funding its development without passing those costs on to customers.

The Security Rating Scorecard was launched in FY 2025. This scorecard provides cleared facilities with a data-driven assessment of their security posture, allowing for more transparent oversight and clear benchmarks for improvement.

To ensure uniform oversight, DCSA launched its Security Academy in FY 2025. It aims to standardize how Industry Security Representatives interact and inspect contractors around the country.

Also in FY 2025, DCSA realigned its Consolidated Adjudications Services to the Working Capital Fund. The shift intended to create a more stable, business-like funding model that scales with the volume of Industry requests.

NISP Policy Advisory Committee Activities in FY 2025

The NISPPAC publicly met once in FY 2025, addressing and discussing issues such as CUI adoption, Cybersecurity Maturity Model Certification, communication channels, training reciprocity, physical security concerns, Sensitive Compartmented Information

indoctrinations, solid state drive sanitization, Insider Threat policies, and physical security policies. In addition to NISPPAC meetings, several committee working groups met, addressing issues such as insider threat, physical security, personnel security, information technology, and advances made with various technological platforms that are key for industry success. The policy working group met several times on a variety of topics. These working group efforts culminated in a series of actionable recommendations. These recommendations underscore the continued commitment of both government and industry to strengthening the National Industrial Security Program in a manner that keeps pace with emerging threats and technological change.

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, guiding the integration of Super Intelligence and emerging

technologies into secure information-sharing environments, the dissemination of policies, and providing analysis of new and continuing insider threat challenges facing the United States government.

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 FY 2025

The SLTPS-PAC met twice in FY 2025, with a primary focus on Department of Homeland Security's (DHS) support for the SLTPS community. DHS is prioritizing enhanced communication and collaboration with all stakeholders. Existing DHS guidance, including E.O. 13549, will undergo a comprehensive internal review, supplemented by input from external partners. DHS is also exploring the establishment of SLTPS subcommittees dedicated to operational issues, with the goal of strengthening interagency coordination and advancing shared mission objectives.



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