ISOO

INFORMATION SECURITY OVERSIGHT OFFICE

2022

ANNUAL REPORT to THE PRESIDENT

WASHINGTON, DC 20408-0001

ISOO's Authorities

- Executive Order (E.O.) 13526, "Classified National Security Information"
- E.O. 12829, as amended, "National Industrial Security Program"
- E.O. 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities"
- E.O. 13556, "Controlled Unclassified Information"
- E.O. 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information"
- 50 U.S.C. 3355a: Public Interest Declassification Board

ISOO'S Mission

- The Information Security Oversight Office (ISOO) supports the President by ensuring that the government protects and allows proper access to Classified National Security Information (CNSI) and Controlled Unclassified Information (CUI) to advance the national and public interest.
- The Director of ISOO receives policy and program guidance from the National Security Advisor, under the direction of the Archivist of the United States.
- We lead efforts to assess the management of classified and controlled unclassified information through oversight, policy development, guidance, and reporting.

ISOO'S Primary Functions

- Recommend policy changes for the CNSI and CUI programs to the President through the Assistant to the President for National Security Affairs.
- Collect and analyze information about the status of agency CNSI and CUI programs and report annually to the President on our findings.
- Develop implementing guidance and approve agency implementing regulations and policies for implementing the CNSI and CUI programs.
- Serve as Executive Agent to implement and oversee agency actions for the CUI program under E.O. 13556.
- Chair the CUI Council under E.O. 13556, the State, Local, Tribal, and Private Sector Policy Advisory Committee under E.O. 13549, and the National Industrial Security Program Policy Advisory Committee under E.O. 12829, as amended.
- Provide program and administrative support for the Interagency Security Classification Appeals Panel (ISCAP) and the Public Interest Declassification Board (PIDB).

LETTER TO THE PRESIDENT

June 5, 2023

The President

The White House

Washington, D.C. 20500

Dear Mr. President,

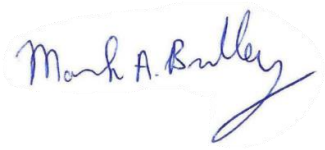
This is my last Annual Report to you before I retire from federal service. I am very proud to have been a career civil servant in the United States government. That said, I leave with a deep sense of uneasiness because so much remains to be done to rethink and to recast the ways we classify and declassify national security information. If we don't change how we do both, our enemies will have an easier time stealing our secrets and many of our citizens will continue to not believe what their government is telling them. Both are threats to our national security.

As I write this, another damaging leak of classified information has come to light. Whether this latest one is a glaring failure of character, a costly breakdown of the systems that are supposed to protect this information, or something else, remains to be seen. This follows on the heels of alleged incidents of mishandling classified information that have drawn enormous media attention on how the executive branch classifies and declassifies national security information, especially at its highest levels. Congress, galvanized into action by these alarming reports, is now teeming with proposed legislation – some better thought out than others – to shore up and fix what many of its members believe are badly broken systems.

In the meantime, I believe we can solve one of our most glaring problems by applying Aristotle's principle that all must be held accountable to the same sets of laws and rules for all those who have access to classified information. This means that even those who are serving in our government's highest offices must follow the same security practices and requirements as the rest of us who have access to this kind of information.

These practices include receiving mandatory yearly training on how to handle, protect, and declassify national security information properly, and attending compulsory exit briefings when security clearance holders leave their federal positions. During these briefings, security officers remind them of their life-long legal obligation to not disclose classified information and to not treat government records, classified or not, as their personal property. I believe that failing to implement this simple recommendation will continue to put our secrets at risk and aid and abet the taking of our country's history. Godspeed, Mr. President.

Sincerely,



Mark A. Bradley

Director, Information Security Oversight Office

ISOO Key Recommendations for FY 2023 and Beyond

1. 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. It is absolutely essential for our national security that this memorandum's goals be met.
2. This memorandum's most important reform centers around E.O. 13526, which governs how the executive branch classifies and declassifies national security information. I recommended several changes to this executive order last year in my Annual Report to you, and I recommend the same changes to you in this year's report. These include:
    a. eliminating the Confidential level of classification so that we can more closely align our classification levels with our approach to cybersecurity domains and with the two-tiered classification systems used by many of our closest allies;
    b. modernizing ISOO's oversight role by updating and streamlining the data agencies are required to report to us;
    c. putting an end to the current automatic declassification system because it cannot keep up with the millions of existing paper records, much less the continuously rising tide of digital CNSI that the executive branch creates every day, making it more than likely that most of these records will never be declassified;
    d. revising the ISCAP's criteria for accepting appeals by prioritizing those of the highest public interest and those of the greatest historical significance.
3. Another challenge the June 2 memorandum addressed is CUI. While I fully support a streamlined and simplified CUI program – the existing program's complexity has crippled its implementation – the executive branch, including the Intelligence Community (IC), must implement this program because eliminating it would threaten our national security. I have seen no other comprehensive alternatives that would sufficiently protect our sensitive but unclassified networks and our sensitive defense technologies, which are constantly being attacked and coveted by our many adversaries.
4. Last year, I recommended reevaluating the criteria for creating and maintaining Special Access Programs (SAPs) and Controlled Access Programs (CAPs) to ensure that they were aligning with our current national security needs and have

the appropriate levels of oversight that they must have. The NSC Staff memorandum addressed the need to tighten how SAPs and CAPs are created and overseen, and I am happy to report that the NSC Staff is leading an interagency effort to push through these reforms.

5. Over this past year, there has been an unprecedented level of focus on the proper handling of classified information and the guardrails, or the lack of them, in place to prevent its mishandling. To discourage future transgressions, including those committed at the very highest levels of our government, I believe that the Executive branch, including the White House and its executive office, need to undergo and require much more rigorous training on how to handle classified information properly. Specifically, I believe the following steps must be taken immediately:

    a. The White House and each agency must review its policies and training materials to make sure that they meet the requirements of E.O. 13526 and that all personnel, no matter their rank, grade or position, take the required information security courses in order to keep and preserve their access to classified information. A greater level of prioritization and attention must be placed on this and there can be no exceptions or exemptions granted to these requirements.

    b. ISOO should work with the interagency to develop these training materials and help train where needed.

    c. Employee out-briefings – including those for the highest level officials – must be robust and include thorough reminders about honoring non-disclosure agreements, submitting items for prepublication review, ensuring all classified information is returned before they leave federal service, and understanding the difference between personal papers and official government records.

    d. The EOP needs to report annually to ISOO on its training programs; certain non-NSC elements of the EOP have resisted this reporting requirement in the past and this must not happen again.

    e. The Classified Outside of Government Program, whose work is discussed later in this report, that my office manages under 32 CFR Part 2001.36(b) provides a critical service on retrieving classified information that is improperly in private hands. We are working on issuing guidance on this critically important subject that has received a significant amount of media attention.

6. If both the PIDB and ISOO are to meet their statutory and executive order requirements, the PIDB must have a separate and additional line item of funding in the annual budget, separate and apart from those of NARA and ISOO. With an overall staffing level of approximately 20, my office's ability to conduct oversight of the CNSI system is hampered by our shared responsibility to support the PIDB. NARA resources are equally stretched thin and cannot support this function under current budgetary allocations.

   Existing models to do this can be found for those used to fund the National Historical Publications and Records Commission and Office of the Inspector General. We feel this is warranted because the PIDB is an independent government board, separate from NARA. It is composed of both presidential and congressional appointees and has a broad mandate to advise and provide recommendations to the President on declassification matters, and to make recommendations to the President about any congressional requests to declassify certain executive branch records.

7. E.O. 12829, as amended, which governs the National Industrial Security Program (NISP), is woefully out of date. President Clinton signed it in 1993. This order no longer reflects current realities and structures nor does it adequately address the keen threats posed to classified information that is held by the private companies that make up our National Industrial Base (NIB). Immediately, this order must integrate into it the CUI program and the 2011 requirements to safeguard networks that store and carry classified information. Likewise, it must modify ISOO's responsibilities and allow the Department of Defense (DoD) to more fully manage the NISP so that it can better defend the NIB and protect it against relentless foreign threats.

8. I am retiring as ISOO's director on June 30, 2023. The White House must move quickly to appoint my successor once it receives the Archivist of the United States' nomination. This appointment is too important to remain unfilled for even an intermediate period of time (which occurred for nearly 12 months in 2016).

ISOO's FY 2022 Annual Report:

Table of Contents

Executive Order 13526, "Classified National Security Information" Program Implementation and Oversight

NSC Staff Memorandum Establishing the Information Management and Classification Interagency Policy Committee (IPC)

As discussed above, the NSC Staff issued a memorandum to agencies on June 2, 2022, establishing the Information Management and Classification IPC process. ISOO participated with senior agency officials in reviewing the overarching objectives for the Information Management and Classification (IMC) IPC and identifying specific tasking and timelines for milestones and overall completion within the IPC.

The IMC IPC is focusing its efforts on classification, declassification, SAPs, and CUI reforms. All of these areas are central to ISOO's responsibilities under Executive Orders and statutes, making ISOO a strong partner for this NSC Staff-led effort.

ISOO's Role in Safeguarding and Declassifying Potentially Classified Information Outside Government Control

32 CFR Part 2001.36(b) provides: "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."

ISOO routinely assists non-governmental organizations and private individuals who discover potentially classified information in their possession. Since the implementation of E.O. 13526 in 2009, we have received more than 80 inquiries from 51 separate institutions and archives from outside the government that potentially possessed classified information. In FY 2022, ISOO received eight such inquires. Three inquires came from individuals who discovered information marked classified dating from the World War II era. In these cases, we were able to determine that the information was no longer classified, and that no further action was needed. An additional five inquires came from non-governmental organizations and archives that house archival collections of former members of Congress, former federal officials, and contractors. In three of these cases, we determined that the records were either never classified or no longer classified. Two other archival institutions transferred records marked at the Secret and Confidential level to us for temporary safeguarding until they can be determined to be unclassified or properly declassified through the mandatory declassification review process.

Interagency Policy Committee Process on Special Access Programs

In July 2021, the NSC Staff tasked ISOO with compiling the first comprehensive list of those agencies with SAPs and CAPs, whether acknowledged or unacknowledged, and to make sure that agencies were following the requirement to establish and monitor these programs, as spelled out in E.O. 13526. Eight agencies reported that they create or manage SAPs or CAPs; however, ISOO identified inconsistencies in compliance and implementation. We believe greater specificity and uniformity in policy and governance, as well as additional oversight and accountability of SAPs, are needed.

Accordingly, ISOO has been participating on a SAP Sub-IPC effort, which focuses on identifying methods to improve and modernize the management of SAPs and CAPs. ISOO fully supports this NSC Staff-led initiative.

Continued Modernizing of ISOO Oversight and Metrics for Analysis

In FY 2018, I directed my staff to develop a more effective way to assess agency CNSI programs by collecting data that was (1) valuable for oversight, (2) mandated to be collected, or (3) helpful to agencies to improve their own CNSI programs. We also streamlined multiple CNSI reporting requirements by consolidating them into one electronic collection request. After a one-year delay due to COVID-19, agencies received the new questionnaire early in 2021, I issued a formal tasking to Senior Agency Officials for the CNSI Program at the end of FY 2021, and all agencies finally completed doing this in early calendar year 2022.

The response to the initial questionnaire was encouraging. Using an electronic portal allowed us to track each agency's progress – or lack thereof, at times – and send them reminders when necessary. Overall, agencies appreciated the ability to send us their data collection requirements online. We also provided a version of the questions that each agency POC could forward around their agency to collect the data required for each question.

My staff analyzed the results gleaned from the first year and applied the lessons learned to the collection for this year. Through careful analysis, we were able to eliminate over 70 questions from the FY 2021 collection whose results were either insignificant or superfluous, reducing the workload on agencies and us. We also modified the questions' format to reduce the number of narrative responses and increase yes/no and numerical answers. This had the positive effect of decreasing our workload while increasing the trackable data we use to monitor the health of the information programs we monitor.

To aid our protracted effort to gain a more accurate cost estimate for the CNSI system, we included three items in the comprehensive data collection questionnaire. First, agencies with declassification programs were asked how many employees were working in each of 12 declassification areas. The total number across the executive branch came to 2,058 employees. This information is further broken down in appendix B. Second, agencies were asked how many employees worked on their CNSI self-inspection programs. We learned that the overall number working in this area across the federal government was 659.

The final element we requested is likely the most demonstrative of the problems we face in receiving reliable data from agencies. They were asked to report on their costs for CNSI security clearance investigations and reinvestigations. Based on their responses, the total number came to just over $714 million for FY 2022. This number is less than half of the amount reported by these same agencies in FY 2021. While it is possible that the money they spent for this did truly decrease by more than 50%, it is more likely that lacking standardized – and Office of Management and Budget-mandated – costing methods, agencies simply counted differently this year than they did last year.

Our reforms continue to be flexible, organic, and open to lessons we learn as we collect and analyze more data. Unfortunately, a number of the least useful data elements that we collect are mandated for agency reporting by either E.O. 13526 or 32 CFR 2001. While we are doing everything possible to decrease the reporting burden on agencies – and the analytical burden on us – until the governing authorities are rewritten, there is only so much these reforms can do.

ISOO Support for the Interagency Security Classification Appeals Panel

I serve as the executive secretary of the ISCAP in accordance with E.O. 13526, and my staff provides program and administrative support. The ISCAP decided upon 21 mandatory declassification review appeals in FY 2022, a significant increase over the previous two years. The increase can be traced to the resumption of in-person ISCAP meetings in April 2022 and to the continued coordination of appeals through a classified network among ISCAP members and staff. The ISCAP administratively closed ten appeals either because they did not meet the requirements for acceptance or because the appellant had withdrawn the appeal. The ISCAP received 19 new appeals in FY 2022, continuing the downward trend of recent years. The backlog of unresolved appeals decreased for the first time, but still numbers over 1,200 appeals.

An analysis of the ISCAP backlog reveals that more than half of the unresolved appeals are because appellants do not receive a response from an agency within one year of its filing. Additionally, the top three individual appellants account for over two-thirds of the backlog. Combining this with the next three most frequent appellants, only six people account for nearly 80% of the total backlog. As Executive Secretary of the ISCAP I understand the importance that each one of these appeals has to the appellants, but I also have a responsibility to prioritize appeals for adjudication and to make the most of the ISCAP's limited resources. I continue to push for changes to our governing authorities that will enable the ISCAP to focus on those appeals of the highest public interest and of the greatest historical significance and not be a body that is monopolized by only a handful of habitual requesters.

Records declassified in full or in part are posted to the ISCAP website at www.archives.gov/declassification/iscap/releases. Significant releases in FY 2022 include the 9/11 Commission interview with President George W. Bush and Vice President Richard B. Cheney, a transcript of an oral history interview with National Security Agency cryptologist Oliver Kirby, and a series of documents from the Central Intelligence Agency concerning support to anti-communist groups during the Cold War.

Original Classification Authority Designations

Due to a reporting error for ISOO's FY 2021 data collection by the Department of State, the OCA count across the executive branch for FY 2021 needed to be amended. Correcting for that error, the numbers for FY 2021 now show that 16 agencies had designated 702 Top Secret level OCAs, 946 Secret level OCAs, and three Confidential level OCAs.

When that error is accounted for, however, there was still a very slight decrease in the number of OCAs across the rest of the executive branch between FY 2021 and 2022. The FY 2022 figures now show that 16 agencies have designated 700 Top Secret level OCAs, 935 Secret level OCAs, and as has now been the case for the past three years, only three Confidential level OCAs. The miniscule number of OCAs at the Confidential level continues to underscore my recommendation from FY 2021 that the Confidential level of classification be eliminated in any future CNSI system.

Security Classification Guide (SCG) Assessments

FY 2022 was the third consecutive year we reviewed a sample of agency SCGs to determine if they are prepared in accordance with E.O. 13526 and 32 CFR Part 2001. We reviewed each SCG in detail, conducting a line-by-line review of the classification tables and examining the introductory and explanatory information in the guides.

During FY 2022, ISOO reviewed 66 SCGs from the following agencies: the Departments of Agriculture, Energy, Health and Human Services, Homeland Security, Justice, State, and Treasury; the Central Intelligence Agency; the National Aeronautics and Space Administration; the National Geospatial-Intelligence Agency (NGA); the National Reconnaissance Office; the Nuclear Regulatory Commission; the Office of Director of National Intelligence (ODNI); the Office of the United States Trade Representative; and the U.S. Agency for International Development. This amounts to just over 3% of the overall number of SCGs.

Of those reviewed, we found that 10 (15.3%) were deficient in listing the appropriate OCA or having the guide signed by the OCA. For the second year in a row, the area where ISOO found the highest percentage of SCGs (35%) out of compliance was in the requirement for listing which classification level applies to each element of information and, when useful, specifies any elements of information that are unclassified. There were once again some deficiencies regarding the requirement to fix a specific date or event for declassification in eight SCGs (12.2%).

The guide from NGA stood out as a model for the future of SCGs. The Consolidated NGA guide – or CoNGA as it is known – includes hundreds of elements from all over the agency and their rationale for classification, all in one central repository. Many elements also include an unclassified version of the information where possible. ISOO commends NGA on this effort and recommends this as a best practice for other agencies to follow.

SCGs remain the cornerstone of a properly functioning classification system because they are the primary tools OCAs use to make their classification decisions. They are also the fundamental tools they use for carrying forward their classification decisions into

derivative classification decisions, which account for the overwhelming majority of classification actions. Deficient or inaccurate SCGs lead to the proliferation of improperly classified information, particularly in terms of precisely stating which elements of information must be protected and at what classification level.

It is clear from our review that agencies must pay more attention to the details spelled out in their SCGs and write guides more accurately and concisely. Consolidation of guides should also be a primary goal, especially at DoD and within the IC.

Fundamental Classification Guidance Review (FCGR)

The FCGR ensures that agency classification guidance is up-to-date and accurate, reflects current circumstances, only authorizes classification in those specific instances necessary to protect national security, and identifies CNSI that no longer requires protection so it can be declassified. Both E.O. 13526 and 32 CFR Part 2001 require agencies with OCA to conduct the FCGR at least every five years and submit the results to ISOO.

For the FY 2022 FCGR, ISOO updated the checklist to require that agencies with OCA identify and report: CNSI that no longer requires protection and can be declassified; SCGs that do not take into account an up-to-date assessment of likely damage to national security if the information were released; consolidation of any classification guidance for specific activities, programs or topics, including Special Access Program (SAPs); and availability of SCGs in electronic and machine-readable formats, as well as the use of electronic marking tools based on metadata standards.

18 agencies completed the FY 2022 FCGR in June 2022. Responses showed a reduction in the number of SCGs because they were canceled or consolidated from 2,460 to 2,116 over the course of FY 2022.

Although agencies continue to reduce the overall number of SCGs, they demonstrate little progress toward consolidating the numerous single-topic SCGs for activities and programs that span offices across the executive branch, including SAPs. Responses did provide new information regarding previously untallied consolidated SCGs, but likely do not reflect the total number of areas where this would be beneficial.

For the FY 2022 FCGR, some agencies engaged their Chief Data Officer (CDO) and Chief Information Officer (CIO), who have been involved in developing standards and policies for the management of information assets in electronic formats. Future FCGRs should expand the scope of questions and engage CDOs and CIOs at every agency with OCAs, to obtain more detailed and precise information about how the increasing volumes of electronic information affect CNSI management.

Although agencies reported a total of 1,897 SCGs in electronic formats, including 503 SCGs in machine-readable electronic formats, agencies differed on what they claimed as electronic and machine-readable SCGs. This is largely because of the lack of a single standard or even consistent guidance defining electronic and machine-readable formats for agencies handling classified information. Similarly, the 13 agencies reporting the use of electronic marking tools inconsistently identified whether these tools incorporated metadata standards in electronically marking classified information.

The adoption of standardized metadata and machine-readable electronic formats will better integrate SCGs across the electronic environment. Agencies must work with OMB to develop workable metadata standards and appropriate guidance on electronic and machine-readable formats. In the absence of federally mandated standards, the Classified Management Tool provided by the ODNI — and reported in the FY 2022 FCGR as in use by the National Security Council and the Department of Homeland Security among others — offers the best example for leveraging existing information technology to improve electronic classification management.

Executive Order 13556, "Controlled Unclassified Information" Program Implementation and Oversight

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. Established in the years following the 9/11 attacks to improve interagency information sharing while establishing consistent, standardized handling safeguards, the E.O. designated the National Archives and Records Administration (NARA) as the Executive Agent for the program, with NARA executing its responsibilities through the Director of ISOO. 32 CFR Part 2002 implemented the CUI program requirements for safeguarding, disseminating, marking, decontrolling, and disposing of CUI.

Interagency Policy Committee Process on CUI

As discussed earlier in this report, the NSC Staff initiated a process to review the CUI program, including E.O. 13556, through the Information Management and Classification IPC. This effort, which is ongoing, is focused on identifying methods to improve and modernize the management of CUI.

Efforts to create a standardized information protection and sharing system for all sensitive unclassified information that the government handles and protects has been a major endeavor requiring significant coordination. Such changes also require strong institutional and program support. My office fully supports and is participating in this IPC process to assist with standardizing and modernizing information security management policies that govern classified national security information and CUI across the executive branch.

Throughout the Information Management and Classification IPC review process, ISOO has instructed agencies to continue to safeguard and handle CUI in accordance with the applicable federal laws, regulations, and Government-wide policy authorities governing this sensitive information. There is much work still to be done, but as a direct result of the years of implementation efforts that have already taken place across the government, we are seeing continual forward movement towards standardization.

CUI Implementation

Finalizing a standard information protection and sharing system for all unclassified information the Federal government protects is extremely complex. The vast number of existing laws, regulations, and government-wide policies that now form the basis of the CUI program were created over decades. Many of these requirements to safeguard and share sensitive information are similar to those for CUI but differ enough from the CUI framework to make the system more complex than would have been possible when creating a new standardized framework. The CUI Registry is the online repository for all information, guidance, policy, and requirements on handling CUI. The Registry identifies all approved categories of CUI, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.

Over the last few years, there have been significant gains in implementing CUI across the federal government. Nearly half of all agencies have published and implemented their CUI policy. Over a quarter of agencies have implemented CUI training programs. Additionally, nearly three quarters of agencies have begun acquiring the funding and resources they need to fully implement their programs. Agencies' progress in this area is included in appendix A.

While there has been significant progress across the government, there has also been a growing interest in identifying methods and strategies to help simplify CUI where possible without sacrificing the integrity of the program. This is a key area of focus within the CUI reform efforts of the IMC IPC.

CUI Data Collection from Agencies

Following the success of ISOO's efforts to modernize the oversight and metrics for analysis of the CNSI program, we created a similar online and electronic approach for annually collecting CUI data. The lessons we learned in implementing the CNSI data collection effort over the last few years proved invaluable because my staff used the same electronic portal and methodology to collect CUI data. Despite the larger pool of agencies that handle CUI – essentially the entire executive branch as opposed to a much smaller group of agencies that handle CNSI – and the learning curve for agencies, the process went extremely well, providing useful data in a more modern and trackable medium. We look forward to continuing to refine this approach.

Federal Acquisition Regulation (FAR) for CUI

We understand from GSA that the CUI FAR clause is currently under review at the Office of Federal Procurement Policy (OFPP). Once that review is complete, the rule will be resubmitted to OMB's Office of Information and Regulatory Affairs (OIRA). It will then undergo the standard process for interagency review.

This clause is a key part of how agencies are going to be able to 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.

The delay in issuing the CUI FAR clause continues to aid and abet in the proliferation of non-standardized approaches by agencies that disadvantage contractors and small businesses, and create gaps in security and reporting. Agencies and contractors repeatedly ask my staff about its status.

Executive Order 12829, "National Industrial Security Program" Implementation and Oversight

As currently structured in E.O. 12829, I am responsible for implementing and monitoring the NISP in consultation with the National Security Advisor. Some of my responsibilities in doing so are developing 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 taking action on complaints and suggestions from persons within or outside the government with respect to the administration of the NISP.

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. It also issues and maintains the National Industrial Security Program Operating Manual (NISPOM), which prescribes the specific requirements, restrictions, and other safeguards necessary under the program. Thirty-nine agencies across the executive branch have classified contracts and are subject to the NISP.

Reforming the Structure of the NISP

The NISP remains in dire need of an overhaul because it is almost 30 years old and no longer supports our national security needs as it should. While I still believe that ISOO has an essential role to play in the NISP, E.O. 12829 requires structural changes to eliminate existing duplication of duties and better align authorities with how the program is being implemented, including strengthening and enhancing DoD's role in the NISP Policy Advisory Committee (NISPPAC). Such changes would also allow us to better allocate our resources to fulfill our core CNSI oversight mission.

Joint Ventures Clarification

In October 2020, the Small Business Administration (SBA) finalized a rule that brought confusion to clearing joint ventures for classified work for the federal government. My office continues to work through these issues.

ISOO Support for the Public Interest Declassification Board

As the Director of ISOO, I serve as the executive secretary of the PIDB in accordance with the Public Interest Declassification Act of 2000, as amended (the Act), and we provide the PIDB with all program and administrative support. The PIDB advises the President on issues pertaining to national classification and declassification policy.

The PIDB began FY 2022 with eight of the nine authorized members. In November, the vacant Presidential appointment was filled by Laura DeBonis. All five Presidential appointments will expire in the first and second quarters of FY 2024. Appointments from the Speaker of the House and the House Minority leader will expire in the 3rd and 4th quarters of FY 2023. Ezra Cohen served as the Chair of the PIDB this year and his term as chair expired January 10, 2023. Vice Chair Alissa Starzak is serving as the acting chair until you appoint a new chair.

The PIDB was tasked in section 1685 of the Fiscal Year 2022 National Defense Authorization Act with conducting a feasibility study of what it would take and cost to carry out a declassification review of federal records relating to nuclear weapons, or ballistic missile tests conducted by the United States in the Marshall Islands, including cleanup activities and waste storage relating to such tests. The PIDB and its staff held over 40 meetings and interviews with stakeholders, including representatives from the Department of Defense, Department of Energy and Department of State, representatives from the Republic of the Marshall Islands, historians, and researchers. The PIDB identified three options for Congress to consider to make additional information available on this important topic. The PIDB delivered their report to the Secretaries of Energy and Defense and the Chairs and Ranking Members of the House and Senate Armed Services Committees in August of 2022.

The PIDB sent you one recommendation in FY 2022. In response to Senator Chris Murphy's 2020 request, the PIDB provided recommendations for the declassification of three documents related to election interference in the 2020 US election and the killing of journalist Jamal Khashoggi. Section 703(b)(5) of the Act provides the Congress with the ability under certain conditions to request the PIDB to review specific records and make recommendations to the President on their classification status, including if they should be declassified. Additionally, the PIDB continues to advocate for additional declassification and maximum transparency to withheld information within the President John F. Kennedy Assassination Records Collection.

My office's administrative responsibilities as the executive secretary of the PIDB continue to require us to divert attention and resources away from our core CNSI and CUI oversight responsibilities. I once again assess that my office cannot effectively continue to support the PIDB under the current statutory structure without substantially more resources.

Executive Order 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities" Program Implementation

The State, Local, Tribal, and Private Sector Policy Advisory Committee (SLTPS-PAC) was established by E.O. 13549 to discuss program-related issues in dispute in order to facilitate their resolution. The SLTPS-PAC – I am its executive secretary – also recommends changes to policies and procedures to remove impediments to the sharing of information under the Program. Since its first meeting in January 2011, the SLTPS-PAC has taken up several issues related to the program's implementation.

In FY 2022, two topics monopolized the SLTPS-PAC's attention: security clearance information and the sharing of cyber threat information. SLTPS-PAC members raised concerns about challenges they faced in obtaining information that their security clearances were verified and in having their clearances passed to other bodies when necessary. We continue to work through these issues in FY 2023.

Appendix A: CUI Policy and Safeguarding Completion by Agency

ISOO developed deadlines with the CUI Advisory Council for phased implementation of the CUI Program at the agency level and issued them in CUI Notice 2020-01. Despite COVID delays, almost all agencies have either completed their agency-level policy or will do so by the end of 2023.

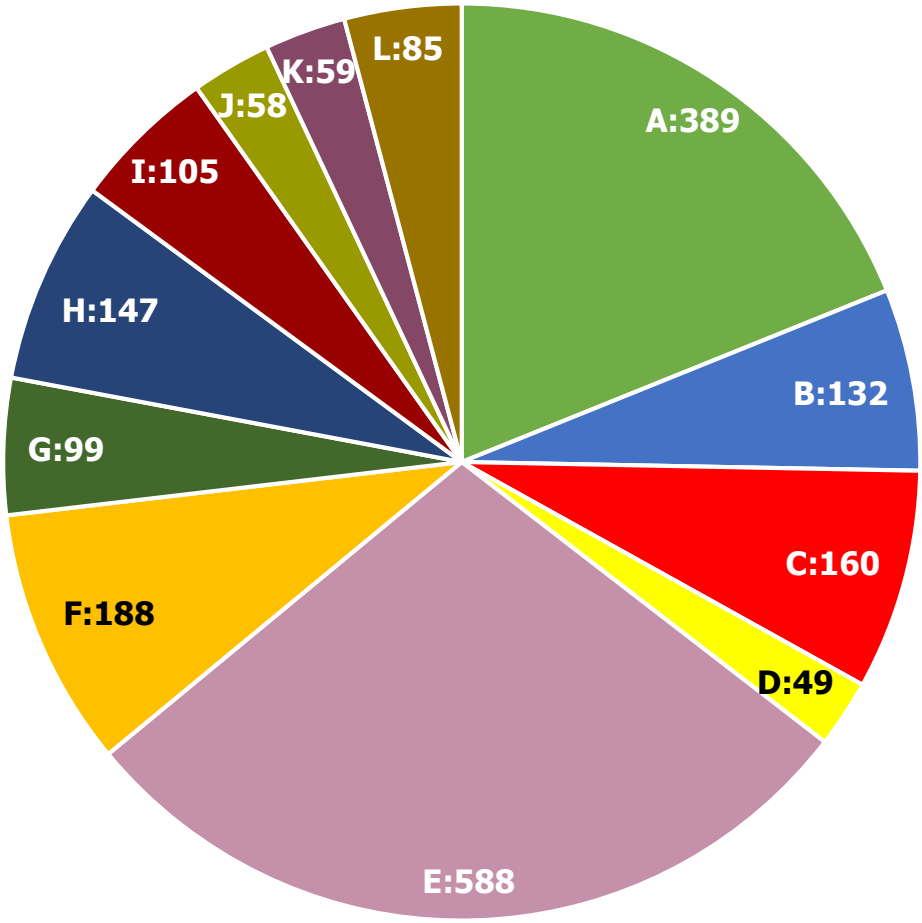
Agency	Policy Status	Safeguarding Status
Ability One Commission	6/30/2023	6/30/2023
Access Board	10/1/2023	Complete
Administrative Conference of the U.S.	9/30/2023	Complete
Advisory Council on Historic Preservation	Complete	10/1/2023
Agency for Global Media	9/30/2023	Complete
Agency for International Development	11/30/2023	9/30/2023
Barry Goldwater Scholarship and Excellence in Education Foundation	Complete	Complete
Central Intelligence Agency	12/31/2025	Complete
Commission of Fine Arts	Not Started	Not Started
Commission on Civil Rights	1/1/2026	1/1/2026
Commodity Futures Trading Commission	9/29/2023	Complete
Consumer Financial Protection Bureau	3/31/2024	12/31/2024
Consumer Product Safety Commission	12/31/2024	12/31/2024
Defense Nuclear Facilities Safety Board	Complete	Complete
Denali Commission	11/30/2023	11/30/2023
Department of Agriculture	Complete	Complete
Department of Commerce	Complete	Complete
Department of Defense	Complete	Complete
Department of Education	Complete	No Data Provided
Department of Energy	Complete	Complete
Department of Health and Human Services	6/30/2023	9/30/2023
Department of Homeland Security	Complete	Complete
Department of Housing and Urban Development	Complete	9/30/2025
Department of Interior	Complete	9/30/2025
Department of Justice	Complete	10/31/2024
Department of Labor	Complete	10/1/2023
Department of State	12/31/2023	Complete
Department of Transportation	Complete	9/30/2023
Department of Treasury	Complete	9/30/2024
Department of Veterans Affairs	8/31/2023	12/31/2024
Environmental Protection Agency	Complete	12/31/2025
Export-Import Bank of the U.S.	6/30/2023	Complete
Farm Credit Administration	Complete	6/30/2023
Federal Communications Commission	9/30/2023	9/30/2023
Federal Election Commission	9/1/2023	Complete
Federal Energy Regulatory Commission	Complete	Complete
Federal Housing Finance Agency	Complete	Complete
Federal Labor Relations Authority	6/30/2023	6/30/2023
Federal Maritime Commission	Complete	Complete
Federal Mediation and Conciliation Service	Complete	Complete

Appendix A: CUI Policy and Safeguarding Completion by Agency, continued

Agency	Policy Status	Safeguarding Status
Federal Mine Safety and Health Review Commission	6/30/2023	Complete
Federal Retirement Thrift Investment Board	Complete	Complete
Federal Trade Commission	Complete	Complete
General Services Administration	Complete	Complete
Institute of Museum and Library Services	6/30/2023	9/30/2023
Interagency Council on Homelessness	12/31/2023	12/31/2023
Inter-American Foundation	Complete	Complete
International Development Finance Corporation	12/31/2023	12/31/2023
International Trade Commission	Complete	Complete
James Madison Memorial Fellowship Foundation	9/30/2023	9/30/2023
Marine Mammal Commission	12/31/2023	Complete
Merit Systems Protection Board	10/1/2024	10/1/2024
Millennium Challenge Corporation	Complete	Complete
Morris K. Udall and Stewart L. Udall Foundation	9/30/2024	9/30/2024
National Aeronautics and Space Administration	Complete	Complete
National Archives and Records Administration	10/1/2023	1/1/2024
National Capital Planning Commission	Complete	6/30/2023
National Council on Disability	12/31/2023	6/30/2023
National Credit Union Administration	6/30/2023	9/30/2023
National Endowment of the Arts	9/30/2023	9/30/2023
National Labor Relations Board	Complete	Complete
National Mediation Board	12/31/2023	12/31/2023
National Science Foundation	Complete	Complete
National Transportation Safety Board	Complete	12/31/2023
Nuclear Regulatory Commission	11/1/2023	Complete
Nuclear Waste Technical Review Board	9/30/2023	Complete
Occupational Safety and Health Review Commission	9/30/2023	9/30/2023
Office of Personnel Management	Complete	12/31/2023
Office of Special Counsel	12/31/2023	12/31/2023
Office of the Director of National Intelligence	No Data Provided	Complete
Pension Benefit Guaranty Corporation	8/31/2023	Complete
Postal Regulatory Commission	6/30/2023	Complete
Securities and Exchange Commission	12/31/2024	12/30/2024
Selective Service System	Complete	Complete
Small Business Administration	10/30/2023	6/30/2023
Social Service Administration	Complete	Complete
Surface Transportation Board	12/31/2023	12/31/2023
Tennessee Valley Authority	9/30/2023	9/30/2023
Trade and Development Agency	6/30/2023	6/30/2023

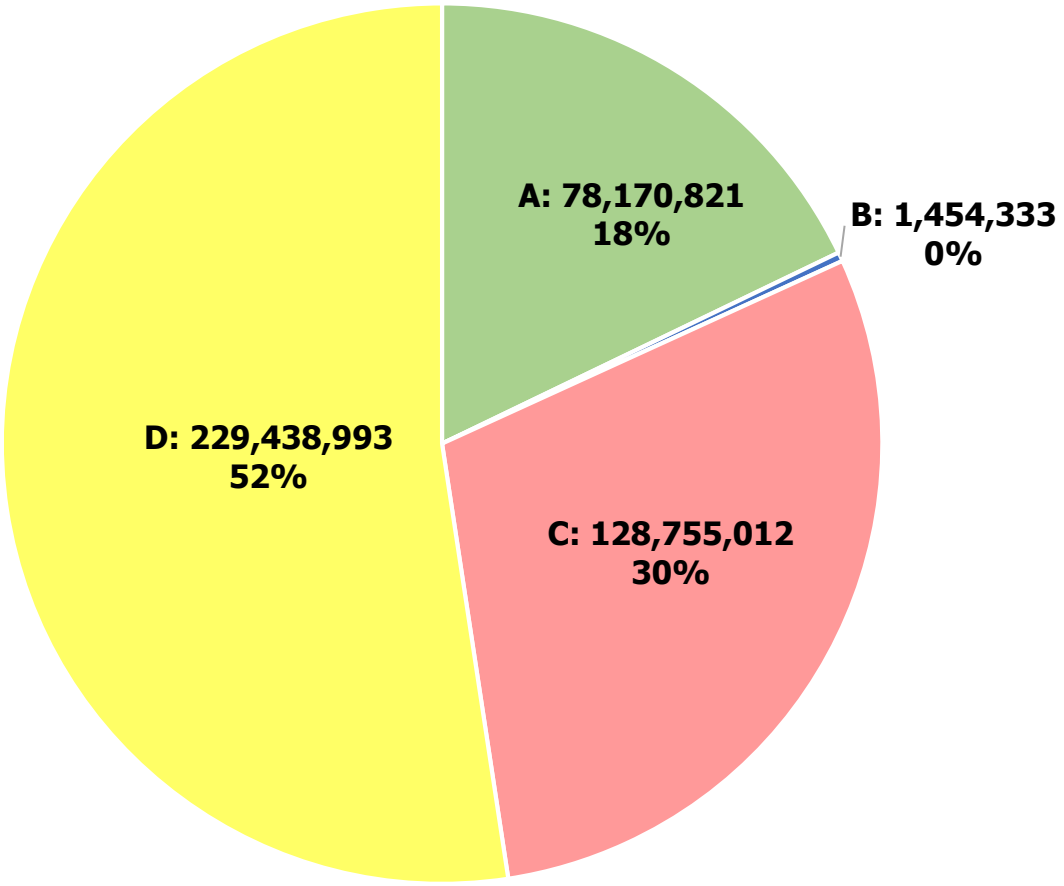
Appendix B: Informational Graphics Regarding Declassification

Total Full Time Equivalent Personnel Working Declassification by Area

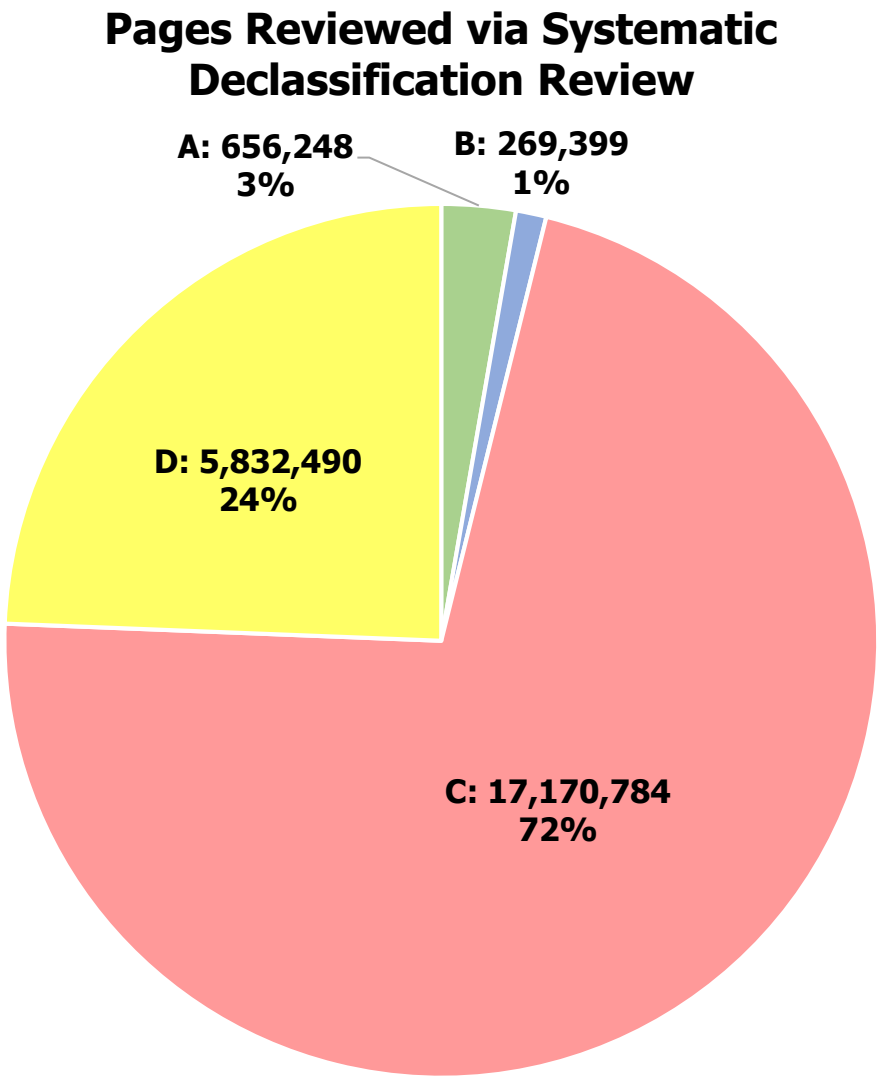


- A = Automatic
- B = Systematic
- C = MDR
- D = ISCAP
- E = FOIA
- F = Pre-Publication Review
- G = Ad Hoc
- H = By Law/Regulation
- I = Court-related
- J = Congressionally-related
- K = NATO/International Use
- L = FRUS

Pages Reviewed via Automatic Declassification

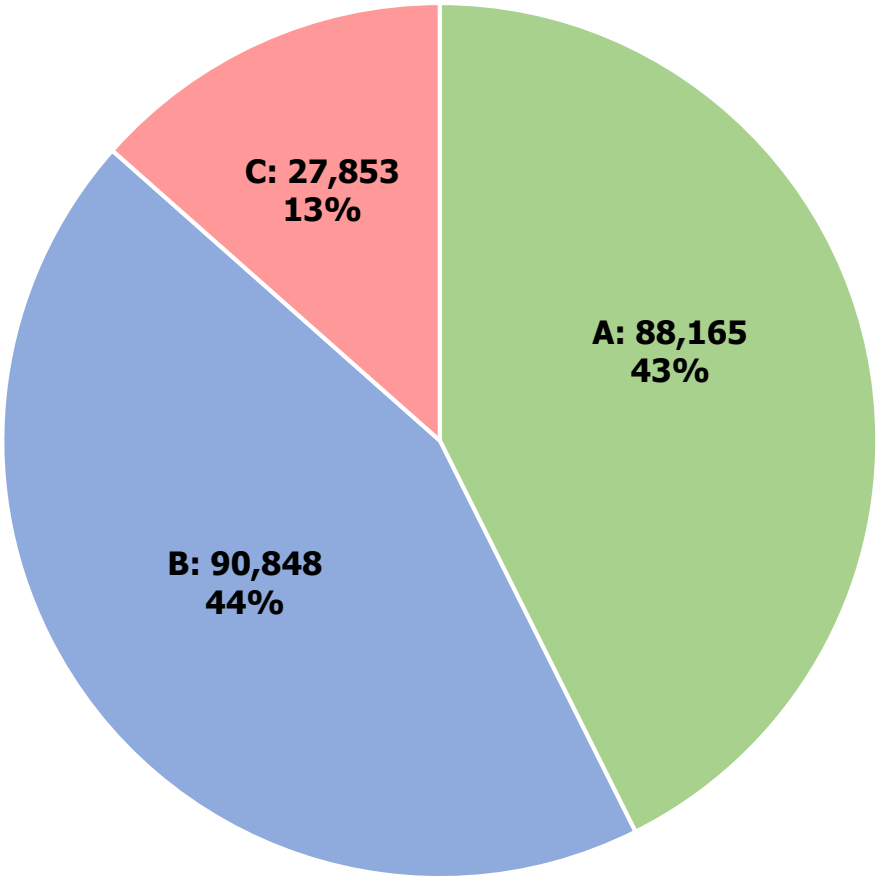


- A = Pages Declassified in FULL via Automatic Declassification
- B = Pages Declassified in PART via Automatic Declassification
- C = Pages Exempted from Declassification via Automatic Declassification
- D = Pages Neither Declassified nor Exempted via Automatic Declassification



- A = Pages Declassified in FULL via Systematic Declassification Review
- B = Pages Declassified in PART via Systematic Declassification Review
- C = Pages Denied Declassification via Systematic Declassification Review
- D = Pages Neither Declassified nor Exempted via Systematic Declassification

Pages Reviewed via Mandatory Declassification Review



- A = Pages Declassified in FULL via Mandatory Declassification Review
- B = Pages Declassified in PART via Mandatory Declassification Review
- C = Pages Denied Declassification via Mandatory Declassification Review