WASHINGTON, DC 20408-0001

ISOO's Authorities

- Executive Order (E.O.) 13526, "Classified National Security Information" (CNSI)
- 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" (CUI)
- 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 and controlled unclassified information 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 classified and controlled unclassified 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 and the Public Interest Declassification Board.

LETTER TO THE PRESIDENT

July 26, 2022

The President

The White House

Washington, D.C. 20500

Dear Mr. President:

As I enter my last year of nearly 30 years of federal service, I believe more than ever that Americans must have faith in their government's honesty and openness. This has become increasingly difficult. We are still emerging from a time when truths were called lies and many of our long-standing institutions and fundamental principles were challenged in ways that we have not seen since the Civil War.

On top of all this, we are still in the throes of a pandemic that has killed over one million of us, and we remain deeply divided politically. Fear and ignorance, the most corrosive and dangerous of all acids for a republic, will continue to eat away at the strength and resilience of our governing pillars if we do not neutralize them with candor and transparency. As Thomas Jefferson observed over 225 years ago, "Whenever the people are well-informed, they can be trusted with their own government."

I believe one of the most effective ways to shore up Americans' belief in their government is to modernize its outdated systems for classifying and declassifying national security information. This is why I was so pleased to receive a copy of the White House's June 2, 2022, Memorandum for Initiating a Process to Review Information Management and Classification Policies, which directs the relevant directorates of the National Security Council to do just that. This could not be timelier because we can no longer keep our heads above the tsunami of digitally created classified records.

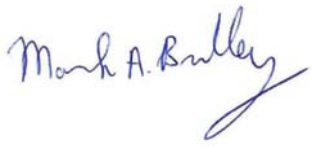
It will be a mammoth task to turn these tidal waves. It will require leadership, doggedness, money, new technology, and an unwavering commitment in the face of

embedded resistance to the core presumption that while we must always protect our national security—the threats we face are real and pervasive—we must do it in ways that recognize, in the words of Senator Daniel Patrick Moynihan, that an era of openness is already upon us and will not accept being rolled back.

My report to you this year highlights the dire need for these reforms and COVID-19's continuing mixed effects on the health of our classification and declassification systems. While the pandemic has caused declassification backlogs to spike and delays to on-site assessments, it has also forced many agencies to become more creative and innovative. Their novel approaches include allowing digital signatures on unauthorized disclosure agreements that meet certain requirements, permitting maximum telework, and overseeing some aspects of their classification programs remotely.

Despite these successes, history remains our best early warning system. It is highly likely that we will experience something like the pandemic again—or something even worse. We must absorb the lessons we have learned so painfully during the past two years and apply them to such future crises. This is especially true in applying them to update our classification and declassification systems and spending the necessary funds to expand and harden our secure communication capabilities.

Sincerely,



Mark A. Bradley

Director

Information Security Oversight Office

ISOO Recommendations for FY 2022 and Beyond

1. Last year, we recommended that the White House aggressively push forward to update the critical national security authorities governing the CNSI system, including Executive Order (E.O.) 13526, "Classified National Security Information," and E.O. 12829, "National Industrial Security Program" (NISP). This is still true. Both contain outdated sections that need to be modernized. Examples of our recommendations for updates include:
    a. eliminating the Confidential level of classification to more closely align with our approach to cybersecurity domains and with the two-tiered classification systems of many of our closest allies;
    b. modernizing ISOO's oversight role by updating and streamlining the data agencies are required to report;
    c. overhauling or eliminating the automatic declassification system as it currently exists, which is unable to meet the requirements for existing paper records and will never keep up with the tsunami of digital CNSI being created daily, making it likely that most of it will never be reviewed for declassification;
    d. revising the Interagency Security Classification Appeals Panel's (ISCAP) criteria for accepting appeals by prioritizing those of the highest public interest and those of significant historical value; and
    e. updating E.O. 12829, which was originally issued in 1993, to modify ISOO's responsibilities and allow the Department of Defense (DoD) to more fully manage the NISP so that its authorities can better defend the United States' industrial base and protect against foreign threats.
2. As part of supporting a modern declassification system, the White House must ensure that modern technologies are applied to it. This process must also move permanently from a paper paradigm to a digital approach for the creation, management, and declassification of CNSI. This should include funding for a fully digital declassification pilot coordinated within the Intelligence Community (IC) by the Office of the Director of National Intelligence (ODNI).
3. All executive branch agencies must fully implement the CUI program. If this program is not fully implemented, we believe the executive branch and its private industry partners will revert to a pre-9/11 agency-centric ad hoc "Wild West" that the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) warned was a risk to national security. The program's demise would also adversely impact other

existing programs such as the National Operations Security Program under National Security Presidential Memorandum (NSPM)-28, efforts to standardize the requirements and protections for this information in government contracts and information sharing agreements that will save the government and private industry money, and undermine Department of Defense initiatives to protect information concerning a variety of advanced technologies. Implementation efforts still require strong White House support, guidance, and direction to make sure the program is fully implemented and adequately funded.

4. The Administration must absorb the lessons learned in the past two years and apply them to develop and implement new, flexible personnel policies and spend the necessary funds to expand secure communication capabilities. Both of these will enhance the abilities of executive branch employees to work remotely with classified information. It is highly likely that we will face something like the COVID-19 pandemic again.
5. Agencies must, to the maximum extent possible, update, correct, streamline, and reduce the number of their security classification guides (SCGs), which are the fundamental building blocks for an accurate and uniform classification system. Ideally, both the DoD and the IC will move towards consolidating their SCGs and will have as few as possible.
6. In response to an NSC request to collect information on the number of active Special Access Programs (SAPs) and Controlled Access Programs (CAPs) that agencies are administering, ISOO identified inconsistencies and challenges to agency compliance with the associated requirements in E.O. 13526 and 32 CFR Part 2001. We recommend reevaluating the criteria for creating and maintaining SAPs and CAPs to ensure they align with current national security needs, and developing and implementing requirements that support national security objectives. Additional oversight of these programs is also necessary to ensure agencies are appropriately establishing and administering them.

ISOO's FY 2021 Annual Report:

Table of Contents

Impacts of COVID-19 on the Classified National Security Information and Controlled Unclassified Information Systems

- COVID-19 continued to impact how executive branch agencies accessed and used CNSI and CUI. Its effects were mixed. On the one hand, the virus forced agencies to scale back their management and oversight of these programs because it disrupted—and in many cases, derailed—their employees' ability to work on and with classified or sensitive information. On the other hand, it pushed several agencies to develop and adopt new practices that should make their management and oversight of these programs more agile and much stronger in the future.
- Significant staffing shortages occurred at the beginning of the COVID-19 pandemic across the executive branch. These were due to numerous employees retiring and to employees not having access to their primary work locations.
- COVID-19 made it difficult or impossible for many federal, state, and local personnel to travel, making it challenging or out of the question to conduct in-person classification reviews and assessments.
- The virus's persistence has continued to make it difficult to obtain Homeland Secure Data Network (HSDN) tokens, Intelligence Community (IC) badges, Personal Identity Verification (PIV) cards, and other security-related items necessary to work in a CNSI environment.
- Likewise, COVID-19 has caused many agencies to hold up implementing physical and information systems safeguarding requirements for CUI. Despite this, about 65 percent, including half of the large cabinet-level agencies, have fully met CUI safeguarding requirements, and another 20 percent expect to do so in 2022. Agency-by-agency progress in this area is spelled out in appendix A.
- In this virulent environment, many agencies were challenged with obtaining in-person signatures. Specifically, the regulations governing signatures on the Standard Form (SF) 312 Classified Information Nondisclosure Agreement prohibited electronic signatures as alternatives to ink signatures. ISOO addressed this issue through a major reform, which is spelled out on the next page.

Agency Adaptations to the COVID-19 Pandemic

- This year agencies continued using many new approaches for dealing with COVID-19–related closures of federal facilities. Most of these applied to their work with CNSI. These included permitting maximum telework, instituting social distancing requirements, following Center for Disease Control (CDC) guidelines, and closing facilities when necessary. Those staff who were required to be on site were able to work on a rotating basis.
- When it was impossible for employees to report in person, agency self-inspections shifted focus to other program areas that could be done remotely. For example, these included reviewing internal security policies and procedures, issuing more internal security notices, conducting more frequent spot inspections, and expanding oversight of classified handling and storage. Some agencies used this pause in activity to update their CNSI policies and to ensure that they reflected up-to-date information security practices.
- Agencies continued to rely on virtual means for their oversight of CNSI programs. Several completely transitioned to virtual self-inspection programs to accommodate social distancing measures and travel restrictions. Several agencies also increased the availability of on-demand and virtual training resources. Some others established new customer service support measures, which provided 24-hour guidance about handling and safeguarding classified materials, equipment, and information.
- One agency, which was building a secure facility, monitored the progress of its construction using video cameras instead of inspectors on the ground. This proved to be an effective method of overseeing a highly sensitive project from afar.
- Given advances in digital signature technologies and their legal validity, we developed a regulatory change that permits certain digital signatures on the SF 312. Our change replaces the previous requirement for wet ink signatures that were much more difficult to obtain during the COVID-19 pandemic. These efforts culminated in a regulatory change to 32 CFR § 2001.80 regarding digital signatures on the SF 312 that removes the prohibition on electronic signatures on the SF 312 and permits agencies to allow for digital signatures that meet certain requirements. We believe this reform—the first substantive change since 2010 to the regulation that governs the entire classification system—is a significant step forward toward modernizing existing requirements and procedures of the CNSI system.

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

Transforming the CNSI System

As spelled out in our recommendation to you in our FY 2020 Report—and again this year—there is an urgent need to update the primary national security authorities that govern the CNSI system. These include E.O. 13526, "Classified National Security Information," and E.O. 12829, "National Industrial Security Program," and their associated regulations because these authorities no longer reflect the system they are governing. My office continues to work with numerous stakeholders to jump-start this effort.

So far, this work has included making a number of recommendations for specific changes to the authorities governing the CNSI system. Examples of our recommendations include eliminating the Confidential level of classification to more closely align with our approach to cybersecurity domains and with the two-tiered classification systems of most of our closest allies, modernizing ISOO's oversight role and process by updating and streamlining the data agencies are required to report, overhauling or eliminating the automatic declassification system as it currently exists so that it can manage the tsunami of digital CNSI being created daily, and revising the ISCAP's criteria for accepting appeals by prioritizing those of the highest public interest and those of significant historical importance.

As part of our recommendations for moving the current CNSI system into a more technologically advanced world, I issued ISOO Notice 2021-03 on October 5, 2021, recommending to federal agencies that they consider using the Technology Modernization Fund (TMF) as a source of funding for cross-agency projects to develop government-wide classification and declassification programs through the use of digital processes and emerging technologies. Congress first authorized the TMF in 2017, then provided supplemental funding in March 2021. In May 2021 the Office of Management and Budget (OMB) and General Services Administration (GSA) updated the rules to allow for partial and minimal repayment of TMF grants for certain projects.

Modernizing ISOO Oversight and Metrics for Analysis

In FY 2018, we began reforming how we collect the data that we use to oversee how agencies manage their CNSI programs. Specifically, I directed my staff to develop a more effective way to measure and assess the health of agency CNSI programs in a way that was less burdensome and yielded accurate data. The information we now gather must be (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 collection request that is now completed electronically, rather than on paper.

While we intended to implement this new questionnaire in FY 2020, we understood the impact that the COVID-19 pandemic had on the agencies' CNSI programs. As a result, we did not deploy our new comprehensive CNSI data collection questionnaire until this year. Agencies received the new questionnaire early in calendar year 2021, and I issued a formal tasking to Senior Agency Officials for the CNSI Program at the end of FY 2021.

One item we removed ended a requirement that agencies count the number of derivative classification actions they made in the past year. With the increased use of electronic classification tools, we have found accurate figures for this number difficult to obtain because of the varied approaches agencies use to estimate the final number of these. One widely used method consisted of asking employees to track their derivative numbers for a week and extrapolate that number for the entire year. This is not a reliable method. Other items removed from the new data collection questionnaire included burdensome and unnecessary details such as how and by whom self-inspections were conducted within agencies and a number of narrative responses that yielded little, if any, useful information.

Additionally, my staff and I determined that the cost information that we had collected about the CNSI system for years was neither accurate nor reliable. We began to remedy this by asking agencies to recalculate how much their CNSI programs cost. We had made some progress in this area, but the COVID-19 pandemic stalled these efforts significantly. Despite this delay, we included three items in the comprehensive data collection questionnaire that we believe will lead to more accurate cost figures about the CNSI system. First, agencies were asked to report on their costs for CNSI security clearance investigations and reinvestigations. Based on 39 agency responses, the total number came to just over $1.5 billion for FY 2021. Second, 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 1,917 employees. This information is further broken down in appendix B. Third, agencies were

asked how many employees worked on their CNSI self-inspection programs. We learned that the overall number working in this area across government was 620.

Our reforms will remain flexible, organic, and open to lessons we learn as we collect and analyze data. We have already identified a number of ways to improve for FY 2022, including eliminating a number of duplicative responses and dropping the requirement for agencies to report their Original Classification Authority (OCA) decisions because we have found those numbers to be inaccurate.

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. While we worked in FY 2021 to reduce the sizable ISCAP backlog of unresolved appeals, a new approach is needed. This backlog is largely the result of a small number of requesters who appeal large numbers of requests that federal agencies were unable to decide within one year. Additionally, the short timelines provided for in the ISCAP's governing regulations leave agencies with little incentive to complete requests on time, resulting in more appeals. I recommend that during the update of critical national security authorities that govern the CNSI system, the ISCAP timelines and criteria for accepting appeals be modified to make them fairer for all appellants. These new criteria should prioritize appeals of the highest public interest and those of the greatest historical value.

The ISCAP decided six mandatory declassification review appeals in FY 2021 and received 41 new appeals, increasing the backlog of unresolved appeals to 1,317. The ISCAP administratively closed 31 appeals, either because they did not meet the requirements of the E.O. 13526 or federal regulation, or because the appellant withdrew the appeal. Records declassified in full or in part are posted to the ISCAP website at www.archives.gov/declassification/iscap/releases.

Digital Signatures and SF 312

In 2021, we began examining the possibility of using digital signatures on the SF 312, the nondisclosure agreement a federal employee must sign before they can have access to CNSI. We did this because the pandemic forced more and more employees with security clearances to work from home; moreover, strides in technology have made digital signatures just as legally reliable as traditional wet signatures. During this process we worked closely with the Department of Justice and the ODNI.

These efforts culminated in a regulatory change to 32 CFR § 2001.80 regarding digital signatures on the SF 312. This change, the first to this regulation in over a decade, removes the prohibition on electronic signatures on the SF 312 and permits agencies to allow for digital signatures that meet certain requirements. When agencies permit electronic signatures on the SF 312, they must use those that (1) are based on public key infrastructure (PKI), which provides the highest levels of security and universal acceptance, and (2) include a reliable certificate authority (CA). The PKI and CA combination ensures authentication (i.e., that the digital signature was made by the person it claims to have been made by), consent (i.e., that the person who digitally signed the form intended to do so), and integrity (i.e., that the SF 312 has not changed since the signature was made).

Security Classification Guide Assessments

FY 2021 was the second consecutive year we reviewed a sample of SCGs to determine if they are prepared in accordance with the requirements of 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.

The DoD is responsible for 73.5% of the 2,116 total SCGs federal agencies use. Over the past two years, ISOO has reviewed 130 SCGs from DoD (6.2% of the overall number of SCGs total). Of those reviewed, we found that 34 (26.1%) were deficient in listing the OCA. All those reviewed provided a date when they were issued or last reviewed. However, 32 (24.6%) had not been reviewed in the last five years, a violation of 32 CFR § 2001.16(a). The area where ISOO found the highest percentage of SCGs (32.3%) out of compliance was in the requirement for listing which classification level applies to each element of information and, when useful, specifying any elements of information that are unclassified. In 18 SCGs (14.6%), the rationale for classification was not provided for some or all the elements of information. There were also multiple deficiencies regarding the requirement to fix a specific date or event for declassification in 27 SCGs (20.7%).

Of significant concern are the 16 SCGs that include 25X exemptions—exceptions to automatic declassification at 25 years that an agency head may authorize when the release of information may reveal certain capabilities or violate a statute, treaty, or international agreement—where the OCA responsible for the SCG does not have the authority to apply such exemptions to newly created documents. DoD should determine the extent to which the deficiencies found in the sample of SCGs reviewed by ISOO are present in other DoD SCGs and identify any actions that must be taken to correct the

deficiencies to ensure that all DoD SCGs provide clear and concise guidance that is in accordance with E.O. 13526 and 32 CFR Part 2001.

SCGs are the primary means for OCAs to make classification decisions and are essential to the proper functioning of the classification system. They are also the fundamental tool used for derivative classification—that is, carrying forward the classification decisions made by OCAs—which accounts for the overwhelming majority of classification actions. When the SCG is deficient or inaccurate—particularly in terms of precisely stating which elements of information must be protected and at what classification level—it leads to the proliferation of illegitimate classified information and enables information to be classified at an inaccurate level. It is clear from the errors we found in our review that agencies must do better. They must pay more attention to the details spelled out in their SCGs. In the future, these guides must be more accurately written, and there must be fewer of them, especially at DoD and within the IC.

Original Classification Authority Designations

The total number of OCAs across the executive branch continued to fall in FY 2021. The FY 2021 figures show that 16 agencies have designated 671 Top Secret level OCAs, 817 Secret level OCAs, and as has been the case for the past two years, only three Confidential level OCAs. The miniscule number of OCAs at the Confidential level underscores the reason why I recommend that the Confidential level of classification be eliminated in any future CNSI system.

NSC Special Access Program Data Call

In July 2021, the NSC tasked ISOO with contacting all agencies with active SAPs and CAPs. Under section 4.3 of E.O. 13526, ISOO has authority to oversee the federal government's SAPs. Specifically, the NSC wanted to compile its 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 laid out in E.O. 13526.

Eight agencies reported that they create or manage SAPs or CAPs. However, in reviewing the responses, 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, is needed.

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 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. While there has been significant progress towards implementing the CUI program across the executive branch, the remaining challenges underscore the program's breadth and complexity.

CUI Implementation

In FY 2016, ISOO worked with agencies and the OMB to develop a CUI budget section within OMB Circular A-11, "Preparation, Submission, and Execution of the Budget." This addition required agencies to submit budget requests for their implementation of CUI. While some agencies have included CUI in their budget estimates to OMB, many still have not. Such a lack of adequate and necessary budget planning will continue to cripple CUI's implementation at those agencies that have failed to do so.

After consulting with the CUI Advisory Council, and with OMB approval, I issued CUI Notice 2020-01, "CUI Program Implementation Deadlines." This Notice requires any agency unable to meet the deadlines for various key CUI program requirements to explain the cause for the delay and what they are doing to comply with the E.O.

Agencies generally report meeting the remaining elements of implementation within one year following the publication of their CUI policies. Over 95 percent of executive branch agencies, including the DoD and the majority of large cabinet-level agencies, reported that they have or will have completed their agency's overarching CUI policy during FY 2022. Agency-by-agency progress in this area is included in appendix A.

The plethora of previously existing laws, regulations, and government-wide policies that now form the basis for the information included in the CUI program were created over decades to safeguard and share sensitive information without consideration for a standardized framework. Many of these requirements are similar to those for CUI but differ enough from the CUI framework—and each other—to make the system

unnecessarily more complex. In an attempt to ameliorate some of this complexity, we are working with agencies to modify many of these regulatory authorities so they align with CUI requirements and reduce the many variations.

Integration of CUI Across Government Initiatives

The principles and policies underlying the CUI program are deeply interwoven into other government programs and initiatives. These include the National Operations Security Program established by NSPM-28, efforts to standardize the requirements and protections for this information in a federal acquisition regulation to be used in government contracts and information-sharing agreements that will save the government and private industry money, and Department of Defense initiatives to protect information concerning a variety of our advanced technologies. The IT systems safeguarding requirements for CUI, established through a collaboration between ISOO and the National Institute for Standards and Technology, also serve as a critical tool for safeguarding our unclassified systems that handle sensitive data. Additionally, consideration for the expansion of the National Insider Threat Program to include CUI pursuant to its definition under E.O. 13556 is well under way, as this gap in the current program has been identified as a key area of concern to our national security.

Federal Acquisition Regulation (FAR) for CUI

We continue to wait, like the Jarndyces in Charles Dickens's *Bleak House*, for the GSA to publish the CUI FAR clause. This clause is a key part of how agencies are going to be able to implement CUI. Once issued, this regulation will standardize the way executive branch agencies enforce the requirements of the CUI framework with nonfederal entities that receive CUI. The CUI FAR regulation was started in 2016 and was dormant at GSA from the fall of 2019 until the spring of 2021.

Since then, we have worked closely with the FAR Council to get the regulation and accompanying documents incorporated into the proposed rule. The lengthy delay in issuing the CUI FAR clause is causing continued non-standardized approaches by agencies that disadvantage contractors and small businesses, and create gaps in system and information security, as well as reporting. Agencies and contractors regularly ask my office about its status and are eagerly awaiting the clause's publication. A final draft of the clause went through OMB and interagency review in March 2022. The FAR Council is adjudicating comments, and once the revisions are approved, we expect the proposed rule will be published for a 60-day public comment period.

Expansion of Insider Threat Program to Include CUI

I continue to believe that protecting CUI from insider threats is critical to the national security of the United States. The scope of the National Insider Threat Program, established by E.O. 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," is limited to only CNSI. It does not include or address current insider threat risks to CUI. My office has worked with OMB and the ODNI's National Insider Threat Task Force to draft a policy to formally allow for, and to govern, the expansion of the National Insider Threat Program that includes CUI and other unclassified critical systems and programs. This policy is undergoing final reviews in both agencies.

CUI and Executive Order 14208, "Improving the Nation's Cybersecurity"

The implementation of the CUI program is a critical component in combating ongoing threats to sensitive unclassified information and is a key part of the response to the goals stated in E.O. 14208. The CUI Program should be regularly integrated into ongoing program developments under E.O. 14208, as well as other similar initiatives, such as those in the recent OMB M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles." Doing so strengthens both, ensures they work fully together for a stronger framework, and facilitates better agency adoption on all fronts. To that end, my staff has reached out to the Chief Data Officers Council and the Office of the Federal Chief Information Officer with recommendations on areas for collaboration and integration.

Information-Sharing Agreements

In addition to sharing CUI with contractors, many agencies must also share CUI with, or receive CUI from, other information-sharing partners. These range from foreign, state, local, and tribal governments to very small organizations and medical providers. The variety and scope of these exchanges is significant. We have been working with agencies to identify these needs as they begin implementing their CUI programs more fully. We have also been working with different agencies and groups of agencies to start developing information-sharing agreements, guidance, and plans for particular situations, including international information-sharing, natural and cultural resources information, and exchanges with tribal governments.

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

Reforming the Structure of the NISP

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.

Like the CNSI system, the NISP requires an overhaul. It is almost 30 years old and no longer supports our national security needs as it should. While I believe that my office has an essential role to play in the NISP because of our oversight responsibilities for the CNSI system, I believe E.O. 12829 requires structural reforms that will eliminate unnecessarily duplicative duties, better align authorities with how the program is in effect implemented, allocate my office's resources most effectively to fulfilling our core CNSI oversight mission, and strengthen and enhance DoD's role in the NISP Policy Advisory Committee (NISPPAC).

NISP Cost Estimation Reform

ISOO continues to chair numerous interagency meetings and working groups to discuss and determine how much the NISP costs the U.S. Government and its partners in private industry. This effort is vital for improving processes and collecting more precise data on how much the federal government spends on implementing the NISP.

NISPOM Update

An arduous multiyear effort to update the NISPOM, led by the DoD, was completed in FY 2021. Cleared contractors had six months to comply with the update to the NISPOM from its effective date of February 24, 2021. The NISP Cognizant Security Agencies (CSAs) provided mission-specific guidance to contractors under their security cognizance on how to comply with the program.

Security Clearance Reform

ISOO continued to solicit from both government and industry stakeholders their feedback in the efforts to modernize security practices and procedures for Trusted Workforce (TW) 2.0, a new approach to personnel vetting that will reduce delays for onboarding new personnel, increase workforce mobility, and provide early detection of risks and threats. As a collaborative partner in TW 2.0, ISOO worked with the Performance Accountability Council—including the ODNI, as the Security Executive Agent, and the Director of the Office of Personnel Management, as the Suitability and Credentialing Agent, to refine and strengthen this new reform.

ISOO Support for the Public Interest Declassification Board

As the Director of ISOO, I serve as the executive secretary of the Public Interest Declassification Board (PIDB) in accordance with the Public Interest Declassification Act of 2000, as amended (the Act), and the ISOO staff provides 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 2021 with only three of the nine authorized members, as the terms of all five Presidential appointments and the Senate Majority Leader's appointment had lapsed. Two Presidential appointees were added in October 2020, namely Benjamin Powell and Michael Lawrence. Paul Noel Chretien was appointed in December 2020, and Ezra Cohen was appointed and named the Chair in January 2021.

The PIDB sent you three letters in FY 2021. The first, shortly after your inauguration, focused on the critical need to modernize the classification and declassification systems, reinforcing the recommendations in the PIDB's report of June 2020. In July 2021, the second letter recommended a prioritized declassification review of records related to the 9/11 terrorist attacks based on their historical significance and public interest. The third letter, dated September 2021, advocated for increased transparency and declassification of CNSI related to President John F. Kennedy's assassination.

The PIDB continued work on a September 2020 request from Senator Chris Murphy to review three specific classified records. 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. While the PIDB accepted the request in FY 2020, COVID-19 proved to be a significant impediment that delayed the review. In addition to secure facility closures, the requirement for new members to obtain all appropriate security clearances further delayed the review. By the end of FY 2021, the PIDB had completed an initial assessment and scheduled meetings with equity-owning agencies. The members anticipate providing their recommendations to you in FY 2022.

My office's administrative responsibilities as the executive secretary of the PIDB require us to divert significant levels of attention and resources away from our core CNSI and CUI oversight responsibilities. With Congress increasingly turning to the PIDB as a preferred vehicle for conducting declassification reviews without any additional funding, the administrative and cost burdens on us have increased significantly over the last several years. I 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 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 implementation of the Program. Early on, topics included the implementing directive for E.O. 13549 and the development of the elements of SLTPS security program, such as training, security compliance reviews, and security clearances. In FY 2021, two topics in particular monopolized the SLTPS-PAC's attention: security clearance information and the sharing of cyber threat information.

Security clearances for SLTPS personnel have been an ongoing topic of concern throughout the SLTPS-PAC's decade of work. During the first several years, clearance discussions centered on the establishment of a central repository for all security clearances granted to SLTPS personnel. Stakeholder agencies agreed that the Central Verification System (CVS) would serve as this repository. Later, there were discussions about whether additional SLTPS personnel needed access to Sensitive Compartmented Information. SLTPS-PAC members raised concerns about challenges they faced in obtaining clearance verification information and having clearances passed to other entities. A working group determined that some agencies were not providing their clearance information to the CVS. Thanks to the efforts of the SLTPS-PAC, one of these agencies began providing this information in 2021, resulting in substantially streamlined improvements to the system and enhancing our national security.

Appendix A: CUI Policy and Safeguarding Completion by Cabinet and CUI Council Agencies

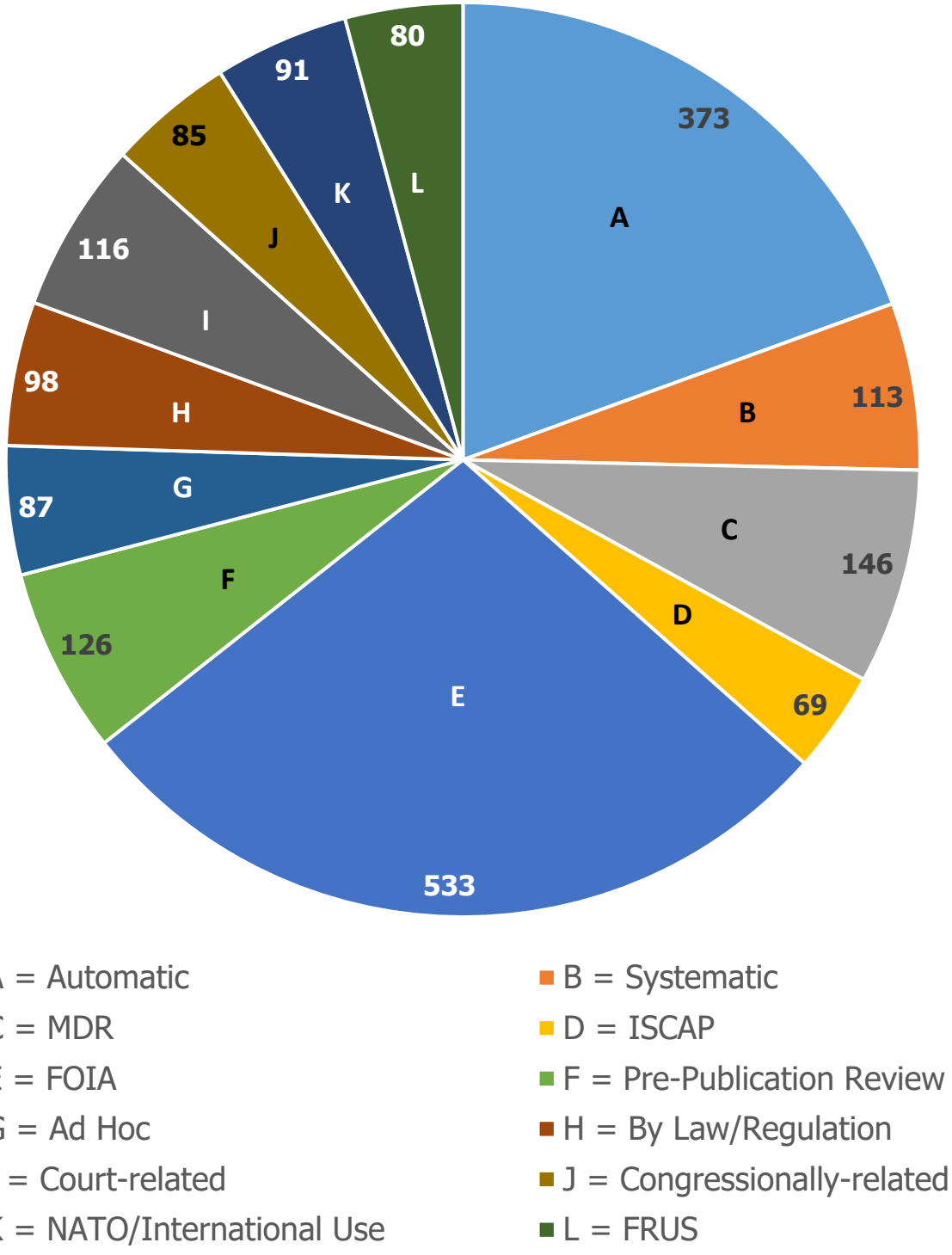
ISOO developed deadlines with the CUI Advisory Council for phased implementation of the CUI Program at the agency level and issued them in CUI Notice 2020-01. Recognizing the impact of COVID-19 on agencies, ISOO provided a grace period to accommodate COVID delays. If an agency was not able to meet a deadline for other reasons, they were required to provide an explanation and an implementation plan to show when they would be in compliance. Despite COVID delays, almost all agencies have either completed their agency-level policy or will do so by the end of 2022. The agencies showing a safeguarding status of yellow have had delays because of COVID, but the majority expect to finish safeguarding implementation by the end of 2022.

Agency	CUI Policy Status	Safeguarding Status
Central Intelligence Agency	Awaiting ODNI	Complete
Department of Agriculture	Complete	9/30/2022
Department of Commerce	Complete	Complete
Department of Defense	Complete	Pending - COVID
Department of Education	Complete	On hold - COVID
Department of Energy	FY 2022*	On hold - COVID
Department of Health and Human Services	Post FY 2022	Post FY 2022
Department of Homeland Security	Complete	Complete
Department of Housing and Urban Development	Complete	12/30/2022
Department of the Interior	Complete	Complete
Department of Justice	1/24/2022*	7/30/2022
Department of Labor	Complete	Post FY 2022
Department of State	Dec 2023 - COVID	Complete
Department of Transportation	12/31/2021*	Complete
Department of the Treasury	Complete	Complete
Department of Veterans Affairs	FY 2021	FY 2023
Environmental Protection Agency	April 2022	12/31/2023
General Services Administration	Complete	7/1/2022
National Aeronautics and Space Administration	Complete	Complete
National Science Foundation	Complete	Complete
Nuclear Regulatory Commission	Complete	Complete
Office of the Director of National Intelligence	12/31/2023	Complete
Office of Personnel Management	Complete	10/2022
Small Business Administration	3/1/2022	9/30/2022
Social Security Administration	Complete	Complete
United States Agency for International Development	April 2022	Complete

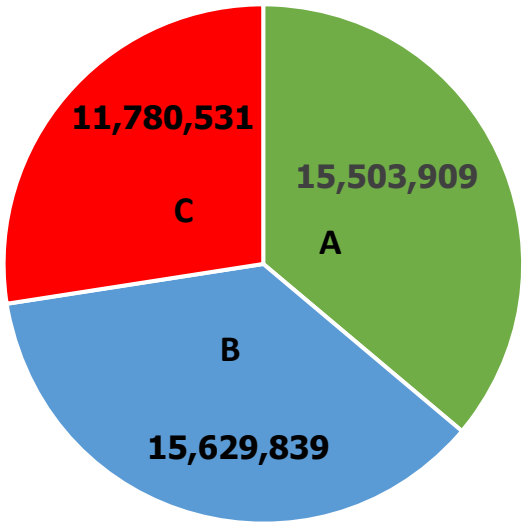
*Note: Since agency submissions for FY21, DOJ, DOE, and DOT completed agency policies.

Appendix B: Informational Graphics Regarding Declassification

Total Full Time Equivalent Personnel Working Declassification by Area

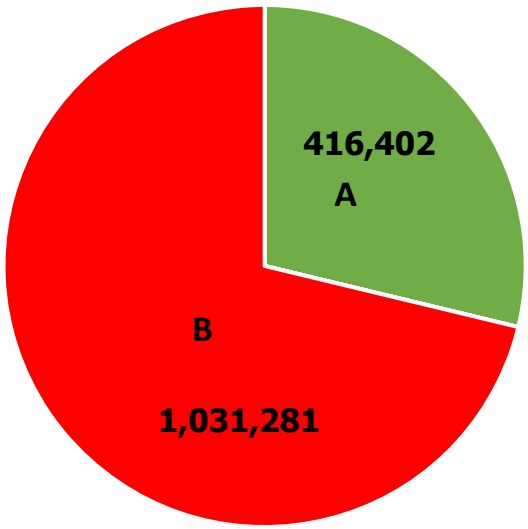


Pages Reviewed Through Automatic Declassification



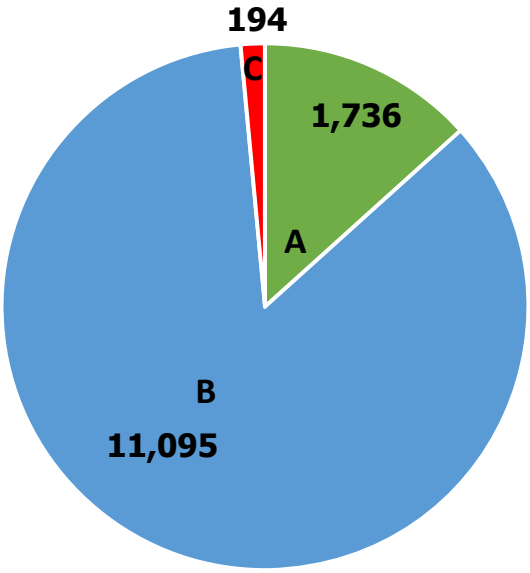
- A = # of Pages Declassified via Automatic Declassification
- B = # of Pages Neither Declassified nor Exempted via Automatic Declassification
- C = # of Pages Exempted from Declassification via Automatic Declassification

Pages Reviewed Through Systematic Declassification Review



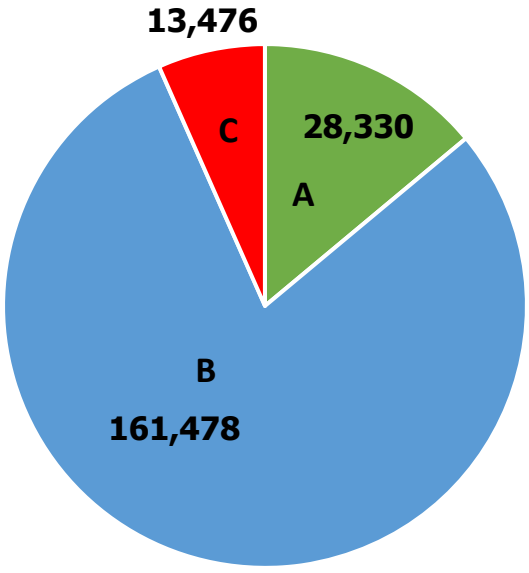
- A = Pages Declassified via Systematic Declassification Review
- B = Pages Denied Declassification via Systematic Declassification Review

Mandatory Declassification Requests



- A = # of Mandatory Declassification Requests Declassified in FULL
- B = # of Mandatory Declassification Requests Declassified in PART
- C = # of Mandatory Declassification Requests Denied in FULL

Pages Reviewed Through Mandatory Declassification Review



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