



2018 REPORT TO THE PRESIDENT



WASHINGTON, DC 20408-0001

AUTHORITY

- 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.”

The Information Security Oversight Office (ISOO) resides within the Agency Services organization of the National Archives and Records Administration. ISOO receives its policy and program guidance from the Assistant to the President for National Security Affairs.

ISOO’S MISSION

We support the President by ensuring that the Government protects and allows proper access to sensitive and classified information to advance the national and public interest. We lead efforts to standardize and assess the management of classified and controlled unclassified information (CUI) through oversight, policy development, guidance, education, and reporting.

FUNCTIONS

- Develop implementing directives and instructions.
- Review and approve agency implementing regulations and policies.
- Review requests for original classification authority and CUI categories from agencies.
- Maintain liaison relationships with agency counterparts and conduct on-site and document reviews to monitor agency compliance.

- Develop and disseminate security education materials for Government and industry; monitor security education and training programs.
- Receive and take action on complaints and suggestions regarding administration of programs established under E.O.s 13526 and 13556.
- Collect and analyze relevant statistical data and, along with other information, report annually to the President.
- Recommend policy changes concerning information security to the President through the Assistant to the President for National Security Affairs.
- Provide program and administrative support for the Interagency Security Classification Appeals Panel.
- Provide program and administrative support for the Public Interest Declassification Board.
- Serve as Executive Agent to implement the CUI program under E.O. 13556 and oversee agency actions.
- Chair the National Industrial Security Program Policy Advisory Committee under E.O. 12829, as amended.
- Chair the State, Local, Tribal, and Private Sector Policy Advisory Committee under E.O. 13549.
- Serve as member of the Senior Information Sharing and Safeguarding Steering Committee under E.O. 13587.

GOALS

- Promote programs for the protection of classified and controlled unclassified information.
- Reduce classification and control activity to the minimum necessary.
- Ensure that the systems for declassification and decontrol operate as required.
- Provide expert advice and guidance to constituents.
- Collect, analyze, and report valid information about the status of agency security classification and controlled unclassified programs.



LETTER TO THE PRESIDENT

August 16, 2019

The President of the United States
The White House
Washington, DC 20500

Dear Mr. President:

Our Government's ability to properly protect and share Classified National Security Information and Controlled Unclassified Information (CUI) continues to face challenges. Thirty years ago, most of this information resided only on paper. The Government stored it in locked safes and shared it in-person by courier or over secure facsimile lines. Today, the Government creates electronic petabytes of classified and controlled unclassified data each month, a deluge that we expect will continue to grow unabated. Digital data now comes in a wide variety of forms, including text, numerical data, and graphical images stored virtually in Clouds and transmitted by email, Instant Messages, and chats.

Information technology advancements have created challenges that inhibit agencies' ability to timely share classified information and CUI among each other, with state, tribal, and local partners, foreign allies, and with the private sector, while still appropriately protecting it. The Government has not invested in the technologies needed to support electronic information management and information security. For instance, it has not spent money on new applications to support precise, consistent, and accurate classification decisions or technologies and processes to prepare for the declassification, decontrol, and public access reviews of large volumes of classified information and CUI in electronic formats.

In my last annual report to you, I made many of the same points. I emphasized that users of this system inside and outside the Government rightly observe that its current framework is unsustainable, and desperately requires modernization. The investment, adoption, and use of advanced technologies lie at the core of this transformation, but we also need new policies and practices that reflect and support the way the Government actually operates in the 21st century.

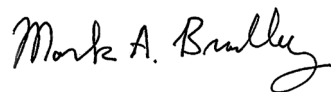
I identified several key shortcomings and provided recommendations that would support modern Classified National Security Information and CUI programs capable of performing effectively and efficiently in the digital age. This letter is a progress report on the steps my office and agencies have taken to implement those recommendations. While there has been some notable progress, I believe this effort will require your continued and sustained leadership, a sizable investment in technology, an integrated “whole of Government” approach, and the support of the executive branch, the Congress, and the public. Even with this level of support, I believe this transformation will take years to implement fully.

The format of this report is different from past Information Security Oversight Office (ISOO) reports. Those reports provided statistical program summaries based on numbers and data that agencies provided to us. I decided to change this format after our office analyzed the data agencies provided. I concluded that we needed new approaches to collect information that are uniform and accurate, and reflect how agencies are actually operating in the digital environment. I believe these new approaches will make our oversight more effective and enhance national security.

ISOO has already begun efforts to reform and modernize our data collection methods, but this will be a multi-year project, requiring significant time, resources, and stakeholder participation. It will necessitate coordination and input from senior White House officials, including staff from the National Security Council and the Office of Management and Budget (OMB), Federal agencies (including their classification program management, chief information officers, records managers, declassification professionals, and public access reviewers), the Congress, the private sector, and the public.

A program report on agency and ISOO actions taken in fiscal year (FY) 2018 is attached, and includes our analysis of progress made on ISOO’s FY 2017 Annual Report recommendations.

Sincerely,

A handwritten signature in black ink that reads "Mark A. Bradley". The signature is written in a cursive, flowing style.

Mark A. Bradley

Director

Information Security Oversight Office

A PROGRESS REPORT

ISOO'S FY 2017 ANNUAL REPORT RECOMMENDATIONS AND FY 2018 PROGRAM ACTIVITIES

Implementing the Controlled Unclassified Information (CUI) Program

Agencies have made positive strides in accelerating their CUI Program implementation efforts. ISOO attributes much of this turnaround to the emphasis placed on the program by the White House and the NSC, as well as recognition of the rising threat environments the Government faces. Additionally, ISOO developed eleven online training modules for agency use and provided them with detailed program guidelines. This extra support helped agencies educate their workforces and begin drafting their implementing policies. ISOO developed standard safeguarding requirements for a Federal Acquisition Regulation (FAR) with support and assistance from the General Services Administration (GSA), the National Aeronautical and Space Administration (NASA), and the Departments of Homeland Security (DHS) and Defense (DOD). ISOO will continue to work closely with these agency partners to finalize this FAR in FY 2019.

Despite some positive strides, ISOO still has concerns. Many agencies are struggling to issue their CUI implementing regulations, submit CUI budget proposals to OMB, implement the program's marking requirements, and staff their agency's CUI Program sufficiently. Solutions to these challenges will require senior agency leadership to prioritize implementing the CUI Program. It will also require procuring automated marking tools and adhering to OMB-mandated guidance regarding CUI budget proposals. ISOO assesses that agencies will not be able to fully implement the CUI Program without dedicated funds and sufficient levels of full-time staff.

ISOO has taken several steps to assist agencies with these challenges. First, we worked with OMB to modify section 31.15 of Circular A-11, *Preparation, Submission, and Execution of the Budget*, to provide additional detailed guidance for agencies to submit CUI budget estimates. The modified guidance reflects that agency estimates should now include hiring staff to manage the CUI Program, develop and deploy automated marking tools, and write internal policies to implement the CUI Program. Second, ISOO formed an interagency working group to develop metadata tagging standards for CUI categories that will facilitate dissemination of CUI to authorized recipients. Third, ISOO enhanced its outreach efforts to aid agency program implementation that included issuing guidance, providing quarterly web-based program updates, and maintaining an active CUI Program Blog. Finally, ISOO focused on providing assistance to individual agencies that requested it.

Transforming the Classified National Security Information System

Modernizing the Classified National Security Information system is a Government-wide imperative. The current system relies on antiquated policies from another era that undercut its effectiveness today. Transforming it will require continued and sustained White House leadership to drive modernization and direct technology investment.

Throughout FY 2018, ISOO gathered information on various agency technology modernization initiatives. Agencies are adopting and using advanced technologies such as Artificial Intelligence, Machine Learning, Continuing Diagnostics and Mitigation, and predictive analytics to support their main missions. Few agencies, though, have contemplated how these technologies could support their Classified National Security Information programs. In meeting with agencies and the private sector, ISOO observed that these technologies remain untapped in this area even as they are deployed for core missions and operations.

Modernizing ISOO Oversight and Metrics for Analysis

In the FY 2017 Annual Report, ISOO highlighted the need to develop more meaningful and accurate metrics to improve oversight. To start this process, ISOO began meeting with agencies to discuss how ISOO could better assist them in improving compliance. ISOO was interested in recommendations for improving agency self-inspection programs, identifying more accurate data assessment methods, and capturing more meaningful metrics.

At the same time, ISOO decided to conduct more targeted reviews of agency programs. ISOO piloted an agency review that focused only on the core Classified National Security Information Program elements that ISOO emphasized in FY 2017 as needing the most improvement: training, classification management, and self-inspections. By limiting the scope of the reviews, ISOO hopes that agencies will be better able to adopt corrective recommendations. These types of reviews show early promise and should allow ISOO to learn more about critical program deficiencies as well as agency best practices. Once identified, these deficiencies and best practices can be used to aid and push the Government's transformation process.

ISOO also took steps to aid interagency discussions on how to improve declassification, and include declassification as part of a technology investment strategy. Declassification remains a resource-intensive paper-based process which lacks modern technologies. For example, many declassification review offices lack the technology to securely transmit records electronically when they contain multiple agency equities that those agencies need to review. Instead, these records are copied and either mailed or delivered by courier. As another example, agencies still sometimes do not know what they previously declassified and later exempt this same information from declassification. Few agencies have the technical capability to identify previously declassified information, much less the staff or time to determine what they have previously released.

ISOO remains committed to assisting agencies to improve their programs and help them prepare for the declassification review of large volumes of electronic records. In FY 2019, ISOO will continue to work through the NSC and with agency partners to promote investment, the adoption of technology, and best practices to aid transformation.

Agency Self-Inspection Reports

Pursuant to E.O. 13526 and 32 C.F.R. Part 2001, ISOO has required agencies to submit detailed self-inspection reports since 2011. These reports include sections allowing for both narrative responses and inputting data. ISOO found that the quality of the narrative responses varied widely, making it difficult for ISOO to effectively oversee and evaluate some agency programs. While some agencies submitted lengthy narratives to reflect how they administer their programs, others did not.

Based on ISOO's analysis of agency self-inspection reports, some agencies have made improvements in critical program areas, such as training. However, some core program areas still require compliance. For example, many agencies have yet to include a critical performance element to evaluate staff whose duties significantly involve creating, disseminating, or safeguarding classified information. This requirement was included in Section 5.4(d)(7) of E.O. 13526 when it was signed a decade ago in 2009.

ISOO is considering changes to the self-inspection reporting process to make it more efficient and effective. Agencies provided feedback that these reports took too much time to compile and complete. The reports also took significant time for ISOO to assess. We are exploring how to reduce the number of narrative responses while also ensuring the report retains its value to ISOO and agencies in assessing program compliance. Possible changes include increased focus on the specific regulatory requirements and working with agencies to develop meaningful and accurate metrics. To streamline reporting, our office is also considering the use of an online platform for agencies to submit their reports. ISOO anticipates this reform effort will continue in the next year.

National Industrial Security Program

The purpose of the National Industrial Security Program (NISP) is to safeguard Classified National Security Information that is provided to United States Government contractors, licensees, and grantees. The NISP executive order established the National Industrial Security Program Policy Advisory Committee (NISPPAC), comprised of both Government and industry representatives, as the official forum to address policy challenges, disputes, and recommend changes.

In FY 2018, ISOO published a revision to the NISP implementing regulation at 32 C.F.R. Part 2004, resulting in improvements to several program areas. The implementing regulation now incorporates Insider Threat Program requirements for the NISP and alleviates concerns that the NISP was not in compliance with E.O. 13587. The regulation also includes additional specificity for processing National Interest Determinations that is meant to increase consistency across agencies and allow for more timely decisions.

In monitoring the NISP, ISOO identified several challenges that must be resolved. For example, one challenge includes the need for the Department of Defense to implement national policy related to foreign contacts and foreign travel reporting requirements. Another challenge is the need for the NISP to integrate policies such as security clearance reciprocity. The resolution of these challenges will improve consistency and efficiency, and reduce costs and delays for both the Government and industry.

Interagency Security Classification Appeals Panel

The Interagency Security Classification Appeals Panel (ISCAP) decided 37 mandatory declassification review appeals and one classification challenge, assessed 23 agency declassification guides, and evaluated for declassification documents proposed for inclusion in the *Foreign Relations of the United States* series published by the Department of State. With the workload of the ISCAP increasing by 106 appeals this year, it continues to seek efficiencies in the prioritization and adjudication of appeals that will lead to the most effective use of its authority to make and to communicate to the public significant declassification decisions. The backlog of unresolved appeals received by the ISCAP at the end of FY 2018 was 1,217 appeals. The ISCAP staff expects the backlog of cases awaiting adjudication to continue to grow in FY 2019. It will continue outreach and education efforts as well as begin corresponding with appellants confirming their interest in remaining in the queue.

For the second year in a row, the ISCAP staff held a public forum that included many appellants and staff from many agency declassification offices. At that meeting, the ISCAP staff shared information about its processes and listened to the concerns of the attendees. It received recommendations and proposals to aid in reducing the backlog. These included limiting the number of appeals an individual may file each year, increasing the length of time that an agency may spend on a request before that request may be appealed directly to the ISCAP, including a member of the public in an advisory capacity on the ISCAP, and placing appeals into different categories of priority for ISCAP review. All of these ideas, as well as the adoption and use of technology in the operations of the ISCAP, remain open for discussion and potential implementation.

Original Classification Designations

The total number of Original Classification Authorities (OCAs) decreased from FY 2017, continuing a longer trend that began in 2009. Agencies reported 715 Top Secret level OCAs, 951 Secret level OCAs, and 8 Confidential level OCAs this fiscal year. While the number of Top Secret OCAs only dropped by one from last fiscal year, the number of Secret OCAs and Confidential OCAs decreased markedly. The number of Secret OCAs dropped by 163, a decrease of approximately 15%. The number of Confidential OCAs dropped from 37 to 8, and only one agency uses delegations of OCA authority at the Confidential level.

