NATIONAL ARCHIVES
ARCHIVES

NATIONAL ARCHIVES *and* RECORDS ADMINISTRATION

2019
REPORT TO THE PRESIDENT

ISOO
INFORMATION SECURITY
OVERSIGHT OFFICE

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 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 Controlled Unclassified Information 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.

NATIONAL
ARCHIVES

ISOO
INFORMATION SECURITY
OVERSIGHT OFFICE

LETTER TO THE PRESIDENT

June 22, 2020

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

Dear Mr. President:

Our Government's ability to protect and share Classified National Security Information and Controlled Unclassified Information (CUI) continues to present serious challenges to our national security. While dozens of agencies now use various advanced technologies to accomplish their missions, a majority of them still rely on antiquated information security management practices. These practices have not kept pace with the volume of digital data that agencies create and these problems will worsen if we do not revamp our data collection methods for overseeing information security programs across the Government. We must collect and analyze data that more accurately reflects the true health of these programs in the digital age.

As a first step, the Information Security Oversight Office (ISOO) engaged extensively this past year with a diverse group of stakeholders and subject matter experts from federal agencies, Congress, and civil society groups to gather their recommendations on data collection reform. The discussions helped to identify specific data that will more precisely measure how robust the Government's national security information programs truly are. I believe many of their recommendations will strengthen our oversight programs and bolster the public's confidence in our work.

After these discussions, I decided to end all outdated and ineffective data and information collections. My office plans to pilot a new data collection questionnaire with agencies in FY 2020. Our questionnaire will streamline previous reporting requirements for classified information by consolidating them into one collection call. It will focus only on data that is valuable for oversight, mandated to be collected in executive order or federal regulation, and that agencies believe is helpful to improve their programs.

My office continued to implement additional changes that I previously set in motion to our inspection and on-site oversight programs. These include a targeted focus on specific elements of agencies' Classified National Security Information programs that have the greatest impact on the protection and appropriate sharing of that information. I found that we previously spent too much time and effort on areas that either did not require in-depth oversight or did not sufficiently improve these programs. In an era where we must strive to make every resource count, I believe this pivot will make our on-site oversight more useful, effective, and cheaper.

A program report on ISOO and agency actions taken in FY 2019 is attached. This includes our analyses of progress made and key actions and judgments in each program area.

Sincerely,

Mark A. Bradley

Mark A. Bradley
Director
Information Security Oversight Office

A Progress Report

ISOO’S FY 2019 ANNUAL REPORT RECOMMENDATIONS AND PROGRAM ACTIVITIES

Implementing the Controlled Unclassified Information (CUI) Program

Key Actions and Judgments:

- ISOO assesses that implementation of the CUI program will play an important role in protecting and sharing sensitive but unclassified Government information across the executive branch. The program requires the establishment of common standards for protecting CUI across the Government. This includes common technical standards to safeguard CUI on both Government and contractor information systems.
- Federal agencies continued to make progress in their implementation of the CUI program in FY 2019. ISOO attributes much of this progress to strong leadership from agency CUI senior program officials. Many agencies reported to ISOO that they will implement their CUI programs by the third quarter of FY 2021, a positive development.
- While there has been progress, implementation has underscored the program’s complexity and real challenges have emerged. I believe that these obstacles will delay some agencies being able to implement their CUI programs. For example, they are facing technical challenges as they begin to integrate CUI marking tools into their information systems.
- Full implementation will require additional resources, including dedicated funds and more full-time staff.

CUI Program Management and Oversight

Executive Order (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. It designated the National Archives and Records Administration (NARA) as the Executive Agent for the program. NARA executes its responsibilities through the Director of the Information Security Oversight Office (ISOO).

ISOO assesses that full implementation at many agencies will require additional resources. In FY 2016, ISOO worked with agencies and the Office of Management and Budget (OMB) to develop a CUI budget section within OMB Circular A-11, *Preparation, Submission, and Execution of the Budget.* Agencies were required to submit budget requests for implementing CUI. While some agencies have submitted CUI budget estimates to OMB, many still have not. This will hinder implementation at those agencies that failed to do so.

Agencies also indicated challenges with disseminating CUI across the executive branch while maintaining CUI safeguarding standards. In response, ISOO formed an interagency working group that is currently developing Government-wide CUI metadata tagging standards to facilitate the dissemination of CUI through Government systems.

I assess that while some agencies will likely be able to implement their CUI programs by the third quarter of FY 2021, others are struggling to do so and will require additional engagement and assistance. For example, my staff and I are working with the Office of the Director of National Intelligence (ODNI) to address CUI implementation issues that are unique to the Intelligence Community. In FY 2020, ISOO issued firm implementation deadlines to facilitate a coordinated transition to the CUI program across the executive branch.

Federal Acquisition Regulation (FAR) for CUI

ISOO continued its work with the General Services Administration, the National Aeronautics and Space Administration, the Department of Defense (DOD), and the Department of Homeland Security (DHS) to develop a FAR for the CUI program. Once issued, this regulation will standardize the way executive branch agencies require non-federal entities to comply with safeguarding requirements for CUI. ISOO expects this FAR to be published by December 2020 after a multi-year development process.

Expansion of Insider Threat Program to Include CUI

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 Classified National Security Information. It does not include or address current insider threat risks to CUI.

ISOO believes that protecting CUI from insider threats is critical to the national interests of the United States. CUI categories such as Proprietary Business Information, Export Controlled Information, and Information Systems Vulnerability Information include sensitive unclassified data that, if compromised, could have significant adverse effects on Government operations and assets. Recognizing these threats, several agencies, including the Federal Bureau of Investigation (FBI), DHS, DOD, and the Department of Health and Human Services' Centers for Disease Control and Prevention, expanded their existing insider threat programs to include CUI. Additionally, several federal contractors in the private sector also expanded their insider threat programs to include CUI. Still, some agencies declined to include CUI in their insider threat programs. These agencies were concerned about additional costs and the lack of a national policy requirement. We are working with OMB and ODNI's National Insider Threat Task Force on examining options for expanding the National Insider Threat Program to include CUI.

Department of Defense CUI Cybersecurity Initiative

The DOD's new Cybersecurity Maturity Model Certification (CMMC) initiative has the potential to aid CUI implementation and improve cybersecurity for Defense Industrial Base (DIB) and DOD contractor systems. The CMMC combines cybersecurity control standards from many different places and unifies them into a single cybersecurity systems framework. This framework uses DOD-accredited independent third-party organizations to conduct network and systems certification assessments of DIB companies. This DOD program is still early in implementation, and ISOO will be monitoring its progress.

Transforming the Classified National Security Information System

Key Actions and Judgments:

- Many agencies have not invested in advanced technologies to support their Classified National Security Information programs. While a number of them are investing in and using advanced technologies to accomplish their agency missions, investments have not transferred down to support the classification system, which remains too antiquated to manage large volumes of classified digital data.
- Classified National Security Information policies and practices remain outdated and are unable to keep pace with the volume of digital data that agencies create. Based on a 'paper' environment, these policies hinder agencies' operations that now rely on advanced technologies and rapid electronic information sharing to accomplish their missions.
- Transformation will require both a "whole of Government" approach across all agencies and a comprehensive investment strategy for developing and using advanced technologies to manage our sensitive Government data, including Classified National Security Information and CUI.
- ISOO saw progress in modernizing policies and processes for obtaining and maintaining security clearances and permitting reciprocity across agencies in FY 2019. New processes, including Insider Threat and Continuous Evaluation, aid information security, accelerate clearance reinvestigations, and reduce delays in processing clearances.
- ISOO's Interagency Declassification Reform Working Group identified 11 different business lines of work that relate to declassification; however, E.O. 13526 only mandates four of the 11, complicating reform efforts.

The Role of Technology in Transforming the Classified National Security Information System

Driven by your Management Agenda, E.O. 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," and other administration information technology directives, agencies expanded their use of advanced technologies and systems in FY 2019. These policies have helped federal agencies become more customer service-oriented, discover efficiencies in processes, and make smart, cost-effective, risk-based decisions to solve complex problems that better serve the American public and help protect our nation. National security agencies and the Intelligence Community are funding and implementing your initiatives. Their transformation includes modernizing networks, developing shared services and applications, and adopting policies and practices to enable secure cloud usage and appropriate information sharing across agencies.

However, agencies have not contemplated the importance of modernizing the Classified National Security Information system in this digital environment. Agencies are not applying or testing advanced technologies that would enable more precise classification and declassification, facilitate information sharing, and improve national security. Classification and declassification actions are still performed manually, which is neither sustainable nor desirable in the digital age. Not only are they inefficient and costly, they are also ineffective and present challenges to properly classifying and safeguarding large volumes of digital data.

IT modernization must expand from supporting primarily agency core mission functions to supporting functions governing information management, including for our classified and controlled unclassified data. The Government also needs new policies for managing large volumes of digital data that protect our national security. Modernization requires both a system-wide approach across agencies as well as a comprehensive technology investment strategy for developing and using advanced technologies to manage sensitive data. These changes will require continued and sustained White House leadership to enable that transition.

Transforming Security Clearance Vetting

There was significant progress in modernizing one aspect of the Classified National Security Information system in FY 2019. Included as Cross-Agency Priority Goal 13 in your Management Agenda, the Security Clearance, Suitability, and Credentialing Performance Accountability Council collaborated with stakeholders and developed new policies that support the needs of national security agencies. This included the transition from periodic background investigations to Continuous Evaluation, the implementation of the National Insider Threat Program, clearance reciprocity across agencies, and new vetting procedures to speed up onboarding. This multi-year effort can be seen as a case study for how to overcome systemic challenges in modernizing outdated policies and practices and investing in technology to support 21st century national security needs.

Declassification Modernization

ISOO established an Interagency Declassification Reform Working Group in FY 2019 as part of its overall data modernization effort. It included representatives from the Intelligence Community, the Departments of Justice, Energy, and State, DOD, DHS, FBI, and NARA. ISOO chose to evaluate declassification processes for several reasons. First, relevant data was available at agencies and this data was consistent and mostly accurate across agencies. Second, both agencies and the public expressed concern about the Government's ability to meet executive order requirements for reviewing large volumes of electronic records. Third, there was public interest and concern about the declassification of Government records.

The working group's first task involved identifying all business lines of work related to declassification, including learning how each is measured, how many agency staff and contractors are assigned to each line of work, and the reasons why each line of work is performed. The working group identified 11 different declassification lines of work, each with its own processes, procedures, timelines, and metrics. However, only four stemmed from requirements in E.O. 13526. The other lines of work are required either by statute (e.g., the Freedom of Information Act), regulation (e.g., Pre-Publication Review), international agreement (e.g., North Atlantic Treaty Organization), or various other mandates (e.g. Court or Congressional requests).

In evaluating all lines of work, the working group noted four similarities that crossed agencies. First, often the same staff was assigned and performed work on several different lines of work. Second, agencies did not have the technology to aid their declassification reviews. Third, agencies are unable to keep pace and are falling further behind mandated deadlines. Fourth, as the volume of records requiring review increases, agencies are making more errors, putting Classified National Security Information at risk and eroding trust in the system.

Modernizing ISOO Oversight and Metrics for Analysis

Key Actions and Judgments:

- ISOO's traditional data collection and oversight activities are outdated and require modernization. Agencies operate differently in the digital age and our data collection and oversight have not kept pace with these changes.
- To address these concerns, we started a multi-year project to modernize our data collection and data collection methods to improve our oversight over the agency Classified National Security Information programs.
- ISOO is piloting a new data collection questionnaire based on input from stakeholders.

Input from executive branch stakeholders included the following criticisms: some of the data was not useful or relevant to managing an agency program, existing forms were burdensome to complete; information was collected on multiple forms on different cycles throughout the year and took substantial time to complete; and some information was duplicative. ISOO also learned that offices responsible for Classified National Security Information programs had experienced budget and staff cuts, and, as a result, their staffs were often assigned additional duties to support other programs or projects. We anticipate that this input, as well as that from congressional and civil society stakeholders, will have a significant impact on data collection reform efforts.

In working with stakeholders to develop the new data collection for use in FY 2020, we focused on data that is valuable for oversight, mandated to be collected under E.O. 13526 or 32 Code of Federal Regulations (CFR) Part 2001, and that agencies believe is helpful to improve their programs. Additional areas for reform included reducing the number of required narrative responses, eliminating duplicative questions, and combining requests that were previously asked in several forms throughout the fiscal year into a single questionnaire that is collected once. We anticipate that the questionnaire will include some elements from the annual self-inspection reporting form, as well as cost data, Original Classification Authority (OCA) reporting, information about the National Industrial Security Program (NISP), and other classification statistics that we have collected from agencies on an annual basis in the past.

ISOO aims to provide the questionnaire to agencies in the third quarter of FY 2020 to allow them sufficient time to review it, ask questions, and seek clarifications before completing it and providing ISOO with their official responses. In FY 2021, we plan to further streamline reporting processes by using an online, digital platform for agencies to report submissions.

Executive Order 13526, "Classified National Security Information" Oversight

Key Actions and Judgments:

- ISOO, because of our limited resources and ability to conduct on-site inspections and reviews, relies heavily on the thoroughness and accuracy of agencies' self-inspection reports in performing our oversight of their Classified National Security Information and CUI programs.
- The major classifying agencies were largely successful in establishing self-inspection programs that included internal oversight, identifying deficiencies, taking corrective actions, and improving their programs.
- Some smaller agencies had insufficient self-inspection programs, and ISOO intends to work with them to improve those programs in the future.
- Compliance with marking requirements for classified information continues to present challenges.
- ISOO continued to use the approach of targeted agency program reviews rather than expansive on-site program reviews.
- We began deploying program analysts to assess agency special access programs (SAPs) in accordance with section 4.3 of E.O. 13526.
- My staff identified a need for targeted oversight of agency security classification guides (SCGs) to improve their utility in making accurate and precise classification decisions.
- Agencies received high scores in declassification assessments that focused on the proper agency application of declassification guidance.
- The total number of OCAs across the Government continued to decrease.

Agency Self-Inspection Reports

E.O. 13526 and 32 CFR Part 2001 require agencies to conduct self-inspections of their Classified National Security Information programs and to report on them each year to the Director of ISOO. These reports include both a description of agency self-inspection programs and the findings resulting from them. These reports provide valuable information for our oversight. Based on our analysis of their reports, ISOO can target both specific agencies where program improvements are necessary as well as specific requirements in the executive order where multiple agencies are deficient.

In accordance with E.O. 13526, agency self-inspections must include a review of a representative sample of their classification actions. This year, agencies reported they reviewed over 200,000 classified products, which included a sampling of records in both physical and electronic formats. The sample size is a tangible example of agencies' commitment to improve their Classified National Security Information programs.

In FY 2019, my staff assessed that the major classifying agencies generally submitted "Very Good" or "Excellent" rated reports according to ISOO-established criteria. They were properly using their self-inspection programs to conduct internal oversight, identify deficiencies, plan for corrective actions, and improve their programs.

Still, we have longstanding concerns about many agencies' compliance with certain elements of E.O. 13526. First, there are too many instances of marking errors within agency samples, including the variety of classified digital data. Second, many agencies have not included a work performance rating measure for personnel whose duties significantly involve creating, managing, or safeguarding classified information. While there was some improvement in FY 2019, the percentage of agencies that report an acceptable level of compliance in these areas is still unacceptable.

In addition, ISOO found that some smaller agencies have self-inspection programs that are insufficient to fully evaluate their effectiveness. ISOO intends to engage with those agencies to improve their programs in FY 2020.

Targeted ISOO Reviews

ISOO's targeted reviews focused only on core Classified National Security Information program elements, including training compliance, classification program management, declassification, and self-inspection programs. This approach aims to enable us to conduct effective oversight with more precision, while reducing the demand on agencies' and our resources. We also continued to conduct follow-up on-site reviews at agencies where significant deficiencies were previously noted to learn if those agencies corrected them.

Special Access Program (SAP) Assessments

SAP information is among the most sensitive classified information that our Government handles. It is essential that agencies manage these programs effectively and in accordance with E.O. 13526 and 32 CFR Part 2001 requirements. ISOO started to plan for its SAP oversight in FY 2018, followed by the deployment of program analysts in FY 2019. Continued oversight is expected in FY 2020. ISOO's oversight methods focus on agency compliance through analyzing agencies' administration of their SAPs. This includes reviewing agency policies, procedures, and processes governing SAP establishment, implementation, management, and internal oversight.

Security Classification Guide (SCG) Assessments

In analyzing agency self-inspection reports, other data call information, and our previous on-site inspections, we determined that there is a need for more comprehensive oversight of agency SCGs. My staff identified several challenges, including SCGs that lacked sufficient specificity to facilitate proper and uniform derivative classification decisions. In FY 2020, ISOO will begin a multi-year oversight project to assess SCGs used throughout the executive branch. The project aims to determine whether SCGs are prepared and updated in accordance with the requirements of E.O. 13526 and 32 CFR Part 2001, and are sufficiently specific to aid in making uniform derivative classification decisions. This new project will allow ISOO to evaluate samples of SCGs from across the full spectrum of defense, intelligence, and civilian agencies.

Declassification Assessments

ISOO assesses annually at least 25 percent of agencies that review a significant volume of records for automatic declassification, focusing on appropriate agency application of declassification guidance. We conducted on-site declassification assessments of five agencies in FY 2019: the United States Army, the Defense Intelligence Agency, the Missile Defense Agency, the National Reconnaissance Office, and the National Security Agency. Under the scoring system that we established in 2012, all five agencies received "High" scores of 85 or above out of 100, and we found only one instance of a missed equity. At one agency, ISOO discovered that the agency reviewed records after the onset of their automatic declassification date. While these records were "newly discovered" by the agency, its program managers did not notify ISOO in accordance with E.O. 13526 and 32 CFR Part 2001.

Original Classification Authority (OCA) Designations

The total number of OCAs across the executive branch continued to decrease in FY 2019. Agencies reported an overall reduction of 89 OCAs from FY 2018 to FY 2019, which represents a 4.9% decrease. This reduction includes a small correction in the overall numbers reported in our Annual Report last year. My staff discovered that the same agencies that ISOO collected and reported data on in previous years did not align with last year's reporting. Accounting for this correction and ensuring that all agencies are now included, the revised numbers of OCAs for FY 2018 are as follows: 748 Top Secret level OCAs; 1,049 Secret level OCAs, and 8 Confidential level OCAs, for an overall decrease of 62 OCAs from FY 2017 to FY 2018. In FY 2019, agencies reported 727 Top Secret level OCAs, 986 Secret level OCAs, and 3 Confidential level OCAs. We believe that the very small number of Confidential level OCAs will likely continue to decrease and we anticipate their elimination in the near future.

Executive Order 12829, "National Industrial Security Program" (NISP) Oversight

Key Actions and Judgments:

- The NISP is outdated and requires modernization, including revisions to E.O. 12829, its implementing regulation at 32 CFR Part 2004, and the National Industrial Security Program Operating Manual (NISPOM).
- The NISPOM policy updating process is too slow, lacking needed flexibility and adaptability to mitigate dynamic threats and vulnerabilities.
- The Government's frequent failure to timely share threat and vulnerability data with cleared industry hinders protecting classified information.
- Executive branch agencies are levying additional requirements on cleared contractors that are not always consistent and are not grounded in policy.
- We saw substantial progress in reducing security clearance backlogs and modernizing vetting processes.

The NISP does not fully address today's threats and vulnerabilities to classified systems and digital data. This must change to adequately respond to these challenges. The NISPOM, first written in 1995 to assist Government and industry with safeguarding Classified National Security Information, is woefully out of date and needs to be rewritten.

We hope that the DOD-led multi-year effort to update the NISPOM will be completed in FY 2020. ISOO judges that efforts to modernize the NISP executive order, its implementing regulation, and the NISPOM would be enhanced by the simultaneous and coordinated modernization of E.O. 13526 and the Classified National Security Information program.

The National Industrial Security Program Policy Advisory Committee (NISPPAC) and its working groups have held numerous meetings that underscored the need to modernize the NISP to detect, deter, and deny contemporary and dynamic threats and vulnerabilities to Classified National Security Information that cleared members of industry have access to. These challenges include threats and vulnerabilities posed by cyber actors, supply chain security, insider threats, risk-based industrial security oversight, and the need to address CUI. Other policy challenges in this area concern security clearance reciprocity, foreign travel and contact reporting, improved policies for security services companies and small businesses, and working with industry representatives earlier in developing oversight policies, methods, and practices.

ISOO will continue to engage both Government and industry stakeholders to solicit their ideas for modernizing security policies, practices, and procedures. ISOO also plans to advocate for more agile NISP policies that effectively address current security threats and vulnerabilities to electronic systems and processes.

Interagency Security Classification Appeals Panel (ISCAP)

Key Actions and Judgments:

- Agency declassification guides have narrower exemptions from previous ISCAP-approved guides. Portions of the guides include common language to increase effectiveness across agencies.
- The ISCAP resolved a declassification dispute between the Departments of Defense and State regarding records proposed for inclusion in a *Foreign Relations of the United States* (FRUS) volume.
- The backlog of cases awaiting ISCAP action continues to grow and most appeals can be traced to agencies' inactions.
- During FY 2019, the ISCAP decided 24 mandatory declassification review (MDR) appeals, approved 23 agency declassification guides, and declassified in whole or in part 60 documents proposed for inclusion in the FRUS series published by the Department of State.

ISCAP Approval of Declassification Guides

The process for completing the declassification guides was lengthy – the ISCAP spent much of its time over the past two fiscal years reviewing them. All 23 agency guides, previously approved in 2012, required extensive changes and resulted in a significant narrowing of information that agencies are authorized to exempt from declassification at 25 years, 50 years, and 75 years. The guides are now more consistent because the ISCAP required the use of standard language in certain sections of all guides. The ISCAP also mandated that agencies handle the same information consistently and uniformly across agencies. This requirement led to agencies working together on shared equity challenges and on developing shared equity guidance in their guides.

ISCAP Support to the National Security Advisor

In FY 2018, the ISCAP received a request from the National Security Advisor to resolve a declassification dispute between the Departments of Defense and State. The Department of State proposed to include 61 documents in the *Foreign Relations of the United States, 1977-1980, vol. IV, National Security Policy*, after its reviewers declassified them, but DOD objected to their declassification. In FY 2019, the ISCAP declassified in whole or in part 60 of the 61 documents at issue. The ISCAP did not review one document as the information in it fell outside the authority of E.O. 13526 and was governed by the Atomic Energy Act of 1954, as amended. The ISCAP's ability to evaluate these documents and make declassification decisions on them demonstrates the role the ISCAP can serve in resolving declassification disputes between agencies.

ISCAP MDR Appeals and Appeals Case Backlog

The ISCAP decided 24 MDR appeals in FY 2019, down from 37 appeals in FY 2018. There were reasons for this decrease. First, the ISCAP prioritized completing the review of agency declassification guides. Second, the ISCAP focused on responding to the National Security Advisor's request and resolving the FRUS declassification dispute. Third, there were two Government shutdowns in FY 2019, including an extended shutdown that led to the cancellation of several ISCAP meetings.

The backlog of MDR appeals awaiting ISCAP decision increased by 36 appeals in FY 2019. The total backlog of unresolved ISCAP appeals increased to 1,286 appeals. The ISCAP staff expects this backlog to continue to grow in FY 2020. Almost all of these appeals can be traced to agencies' inaction and inability to review MDR requests within the one-year timeframe provided for in 32 CFR Part 2001.