NATIONAL ARCHIVES *and* RECORDS ADMINISTRATION

2020
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 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 24, 2021

The President
The White House
Washington, DC 20500

Dear Mr. President:

The year 2020 was like no other in the history of our country's Classified National Security Information and Controlled Unclassified Information systems. The COVID-19 pandemic has been a stark reminder that we really do not know what life has in store for us around the corner. It also gave us an object lesson in what happens when many of our Government's activities are stopped or slowed to a crawl, but it also provided us with a vivid demonstration of our federal workforce's extraordinary capacity to adapt and function in the wake of an unprecedented crisis.

The pandemic adversely affected every aspect of our Classified National Security Information and Controlled Unclassified Information systems. It shuttered buildings, limited or prevented access to classified networks, forced many federal workers to telework or work remotely, delayed the modernization and deployment of badly needed technological updates, crippled oversight efforts, and dramatically slowed the declassification of historically important records, increasing an ever-expanding backlog.

Despite these obstacles, many agencies rose to the challenge. Some formulated and adopted new policies that permitted their employees to work with lower-level classified information in their homes. Others consciously decided to keep as many of their work products as possible unclassified. Without access to classified information while working at home, their employees improvised and developed unclassified substitutions for classified products to share more information with their colleagues and policymakers. Several agencies plan to make these innovations permanent.

While these modifications are commendable, they fall short of solving some of the most glaring inadequacies that the last year has exposed. Above all else, the pandemic underscored the need to rethink, update, and strengthen several of the key policies and authorities that undergird these critical information programs. I strongly urge you to task your National Security Advisor to undertake a comprehensive examination of these in the pandemic's wake, reforming those that are outdated or need to be modernized in the face of new challenges. If the White House does not rapidly make progress in these areas, I strongly believe that Congress will continue to advance efforts to patch these shortcomings through legislation in what has traditionally been an executive branch arena, which may raise some thorny constitutional issues.

Sincerely,

Mark A. Bradley

Mark A. Bradley
Director
Information Security Oversight Office

Table of Contents

ISOO'S FY 2020 ANNUAL REPORT: RECOMMENDATIONS AND PROGRAM ACTIVITIES

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

Key Actions and Judgments:

- The COVID-19 pandemic has significantly slowed the U.S. Government's efforts to modernize and reform the Classified National Security Information (CNSI) system.
- Increased telework and remote work are fundamentally altering the way the U.S. Government's employees and contractors are accessing and using CNSI and Controlled Unclassified Information (CUI).
- Agencies' management of their CNSI programs, as well as our oversight of them, was also disrupted and scaled back because of the COVID-19 pandemic.
- The COVID-19 pandemic has greatly impacted agencies' abilities to complete required automatic declassification reviews, decreasing the volume of classified information that will be declassified and increasing backlogs of Mandatory Declassification Review (MDR) requests.
- The COVID-19 pandemic has forced agencies to adapt and modify their CNSI and CUI programs, resulting in them developing and implementing new practices that may make them more agile in the future. For example, many agencies were forced to modify their CNSI self-inspection processes, with some reporting that they plan to continue using these modified processes when their normal operations resume.

COVID-19 Pandemic Impact on CNSI System Modernization

The COVID-19 pandemic has significantly delayed the U.S. Government's efforts to modernize and reform the CNSI system and stalled the National Security Council's (NSC) plans to update and revise several of the critical policies that govern it. Some agencies were able to adapt and innovate independently to continue their missions, while others, typically those whose missions are less focused on national security, de-emphasized their CNSI programs. While some of these independent agency efforts were positive developments, we assess that a comprehensive whole-of-government approach is needed.

Several agencies were beginning to make progress in developing advanced technologies for their declassification programs, but the pandemic stalled their efforts. Once modified pandemic operations end, we strongly recommend that agencies consider how best to leverage federal initiatives such as the Technology Modernization Fund, authorized by the Modernizing Government Technology Act of 2017, to apply for funds to promote cross-agency information technology modernization projects that will improve their classification and declassification programs.

A Changing Work Environment for CNSI

The CNSI system has long been governed by the basic rule that personnel with security clearances access classified information in secure office spaces. This premise began to shift once agencies realized that the COVID-19 pandemic was not going to be just a short disruption to their operations. Agencies realized that their employees were going to have

only limited, or in many cases, no access to secure facilities for an extended period. Faced with that stark reality, agencies began rethinking long-standing policies to address this unprecedented challenge. These efforts included formulating and adapting procedures to permit their employees to work with lower-level classified information in their homes. For instance, one large agency developed detailed requirements and policies, including mandatory oversight, system security, and accountability plans, so that their more senior employees could work on Secret and Confidential level information in their homes. If successful, we believe these individual pilot projects might well pave the way for comprehensive plans to permit a federal workforce working remotely to access, use, create, and share classified information.

We also received information that teleworking employees at some national security agencies have consciously decided to keep their work products unclassified. Without access to classified information while working from home, these employees improvised and developed unclassified substitutions for classified products so that they could share information with colleagues, including others who were teleworking. For example, one agency comprehensively reviewed all of its classified training products and created new unclassified substitutions for 41% of those products. Another agency directed its employees to make every effort to keep their work unclassified. These policies and efforts were always coupled with upgrades in the security of information networks and systems.

Designing and implementing new security policies and procedures that operate more effectively and efficiently in the digital environment to permit improved secure teleworking and remote work are now more important than ever because of the potentially high risks both pose to CNSI from hackers and bad nation-state actors.

Agency CNSI and Self-Inspection Program Reporting during the COVID-19 Pandemic

Many agencies reported to us that the COVID-19 pandemic adversely affected their CNSI program management and oversight abilities. To both increase our understanding of pandemic-related burdens and to help alleviate demands on time related to standard annual reporting requirements, in accordance with Office of Management and Budget (OMB) COVID-19 guidance, we tasked agencies in FY 2020 with an abbreviated CNSI data collection.

Our FY 2020 data collection included questions covering the COVID-19 pandemic's impact on the management of agencies' CNSI programs, including on their self-inspection programs. Agencies were also asked to describe any special measures they had taken and any best practices they had developed for conducting effective CNSI program oversight during the pandemic. Out of concern that agency security resources were already strained, and to help ensure that agencies could most effectively direct their resources to the management and oversight of their CNSI programs, we did not ask agencies to submit the comprehensive self-inspection reports that we required over the previous nine years.

As we expected, nearly all agencies reported that the COVID-19 pandemic disrupted the management of their CNSI programs. Extended facility closures, limited building access, and maximum teleworking required agencies to change how they implemented various aspects of their CNSI programs. Two of the most impacted areas were declassification and self-inspections.

Most agencies were unable to review a significant quantity of classified records for automatic declassification or those that were requested under Mandatory Declassification Review (MDR). A few agencies reported that their declassification programs were curtailed because they were dependent on their access to the National Declassification Center (NDC) or the Washington National Records Center (WNRC), which were closed due to the pandemic. Nevertheless, some agencies reported that they were still able to meet their declassification milestones.

Just over one quarter of agencies reported that they did not conduct any self-inspections at all, and nearly 30 percent of all agencies indicated that they did not cover all the required elements of their self-inspection programs because of no or limited access to their facilities. Despite this, nearly all agencies that manage significant CNSI programs reported to us that they conducted self-inspections. A few even submitted summaries of their findings in all program areas.

As alternatives to on-site reviews, many agencies relied on electronic communications and the use of virtual platforms. They performed remote security compliance reviews and used data requests to gather self-inspection data. Several agencies identified some of their alternative measures as best practices. These encompassed remote or virtual compliance reviews, electronic self-inspection forms, robust data requests for remote evaluations, and standardized forms for interviews. Some agencies told us that they intend to continue to use these measures to supplement on-site reviews when their operations return to normal.

Facility closures also negatively affected many agencies' abilities to instruct new employees on how to access CNSI. New hires at several agencies were unable to physically sign the Standard Form 312, Classified Information Nondisclosure Agreement. Closures also impacted some classified systems that required additional maintenance because of long periods of non-use; some users lost access altogether and were often delayed in having their access reestablished.

Most agencies' CNSI training programs were unaffected because they were already delivering their courses online prior to the pandemic. Other agencies, in response to the pandemic, increased their online training capacity and adapted their training procedures to fit this new paradigm. Still, a handful of agencies told us that they could not provide some of their more specialized training.

No agency reported to us that the pandemic caused any mishandling of classified information or security violations, nor did we receive any notifications of investigations. Although the pandemic limited access to CNSI and caused agencies to modify elements of their programs, we are not aware of any instances where it caused classified information to be placed at risk.

The pandemic did force agencies to innovate and reassess certain information security policies so that their employees could remain focused on their missions. Agencies developed alternative schedules that included working in shifts and limiting in-person staff contact. They upgraded their telework capabilities and worked with chief information officers, chief information security officers, and systems designers to ensure that these systems were adequately protected by strengthening access permissions. Several agencies also updated their telework policies, which reminded their employees that they were expected to follow and obey all operational, cyber, and physical security requirements.

We believe that agencies should use lessons learned from the pandemic to continue to adapt and modernize operations through adopting new policies and procedures for a more agile, digital-based system that is better situated for 21st century national security missions. We also believe a coordinated approach to modernizing policies and practices, led by the NSC, is the best way to enact needed changes to the CNSI system.

As outlined in the *"Modernizing ISOO Oversight and Metrics for Analysis"* section of this report, ISOO also plans to roll out a new agency reporting questionnaire this year to monitor agency progress. This reformed questionnaire will include revised self-inspection reporting questions.

COVID-19 Impacts on Agency Declassification Programs

The COVID-19 pandemic significantly eroded many agencies' abilities to complete automatic declassification reviews as required in section 3.3 of E.O. 13526 and further increased backlogs of MDR requests.

Immediately following the declaration of a national emergency on March 13, 2020, all agencies shut down their declassification programs after closing their on-site facilities, and the NDC and WNRC closed. These programs were largely deemed 'non-essential' as national security agencies tried to limit their number of on-site employees to the minimum necessary to accomplish their core missions. Beginning in the summer, several agencies permitted a small number of declassification program employees to return to their facilities part-time so that they could perform the classified work that they could not otherwise do by teleworking. By September 2020, most agencies permitted part-time work and staggered schedules to allow more of their declassification employees to return to their secure facilities.

Still, agencies began contacting us in August 2020, asking about delaying the onset of automatic declassification, or requesting such a delay. In response, we sent agencies an informal questionnaire that we developed to learn about the impact of the pandemic on their declassification programs and on what challenges they were facing. The questionnaire included four questions about the status and progress of automatic declassification reviews and one question about the status of MDR programs.

We sent this questionnaire to 31 agencies, including eight combatant commands. Twenty-three agencies responded. Overwhelmingly, we found that most agency programs were greatly impacted by the nationwide closures, including the NDC and WNRC, and restrictions in place. Most responding agencies indicated that they would be unable to complete their automatic declassification review of records by the December 31, 2020 deadline. Only four agencies answered that they would be able to complete their automatic declassification reviews on time.

While agencies indicated they either already had, or expected to, complete the automatic declassification review of approximately 40 million pages of records by the December 31, 2020 deadline, they also reported that they would not complete declassification reviews on approximately 23.6 million pages by the deadline, though one agency accounted for 80 percent of this backlog.

Most agencies noted multiple challenges, including lengthy facility closures, the inability of supporting staff to enter facilities, diminished on-site staff availability, and position vacancies. Some agencies cited factors external to their organizations. For instance, several reported that once they had a sufficient number of employees to perform the work, they were unable to retrieve and access their records stored at external facilities, such as the WNRC, which remained closed. Other agencies highlighted the extended closure of the NDC. These agencies were unable to conduct automatic declassification review of their records, review referrals, or conduct Quality Assurance/Quality Control (QA/QC) reviews.

The processing of MDRs also suffered during the pandemic. While agencies received fewer requests than in FY 2019, backlogs and delays nevertheless climbed. Agencies reported that they prioritized the processing of Freedom of Information Act (FOIA) requests above processing MDR requests. They explained that FOIA legal requirements and deadlines remained firm despite the pandemic, and opted to assign their returning employees to process FOIA requests. Typically, agencies logged MDR requests, assigned a case number to each, and informed the requester of receipt and the case number, but did no further processing.

We engaged with the NDC, the National Archives and Records Administration (NARA)'s General Counsel, and the NSC to discuss the agencies' concerns and identify possible solutions that would conform to requirements in E.O. 13526 and its implementing regulation. We used the data compiled from the questionnaire to help inform this discussion.

We and the NSC determined that E.O. 13526 and its implementing regulation did not allow for a delay in extending the automatic declassification deadline, nor did either permit a waiver for agencies to rely on so that they could review these records after the deadline. On November 20, 2020, we issued a memorandum to all senior agency officials informing them of this determination and advising them that automatic declassification programs should prioritize records for review by adopting a risk-based approach. We also told agencies to focus their automatic declassification reviews on their most sensitive records and those with the highest levels of classification.

This particular impact of the COVID-19 pandemic will likely affect both agencies' and the NDC's operations in FY 2021 and for years to come. The automatic declassification provision in E.O. 13526 only applies to the information of the originating agency; it does not apply to information embedded in records that other agencies created. Thus, agencies must still identify other agency equities, as well as Restricted Data/Formerly Restricted Data in records that were not reviewed before the December 31, 2020 deadline. These requirements will delay the accessioning of records to the NDC until those reviews are completed. Additionally, NDC QA/QC processes will likely be more time-consuming. This will almost certainly hold up making these records available to the public.

COVID-19 Pandemic Impacts on the Interagency Security Classification Appeals Panel

The COVID-19 pandemic adversely impacted and significantly degraded the Interagency Security Classification Appeals Panel (ISCAP)'s ability to perform its mission. The ISCAP, established by E.O. 13526, is a Presidential appellate panel empowered to decide certain classification and declassification issues. These include MDR and classification challenge appeals, as well as agency exemptions from automatic declassification.

The processing, review, and adjudication of classified records, which accounts for a substantial amount of the ISCAP's work, cannot be done remotely. Facility closures, including complete closures for extended periods of time, limited access to secure workspaces. Additionally, the pandemic led to new competing priorities in allocating the time of specialized declassification employees who work on the ISCAP's appeals.

Nevertheless, the pandemic forced one badly needed reform. Before March 2020, the ISCAP's MDR appeal adjudication process was largely paper-based. When limited operations resumed in the summer of 2020, one ISCAP staff member was able to begin working part-time in the ISCAP's secure workspaces, which helped to increase productivity. This staff member developed new procedures for resolving ISCAP appeals electronically by using a classified network. The ISCAP will continue to refine its procedures, with the goals of focusing its attention on significant declassification decisions and using technology to streamline the processing and adjudicating of appeals.

Despite this, major challenges for the ISCAP remain. Only one ISCAP staff member at ISOO is currently able to work on classified materials. Additionally, some ISCAP member agencies do not have ready access for their ISCAP members and staff to the classified network that enables electronic resolution of appeals. Our ISCAP staff also does not have secure video teleconferencing capability, which prevents the ISCAP members and liaisons from meeting securely through that method. We continue to advocate for funding to address these technological limitations.

Transforming the Classified National Security Information System

Key Actions and Judgments:

- The White House must begin a comprehensive interagency process, led by the NSC's Records Access and Information Security directorate, which has wide experience in coordinating and managing classification and declassification programs across the federal government, to review and update critical national security policies and authorities that govern the CNSI system. These include Executive Order 13526 "Classified National Security Information" and Executive Order 12829 "National Industrial Security Program" (NISP), which both contain several sections that are outdated and need to be modernized. If it does not, we believe that Congress will continue trying to satisfy these needs legislatively.
- Congress spearheaded two significant modernization developments in FY 2020: (1) the FY 2020 National Defense Authorization Act (NDAA) included several provisions supporting CNSI modernization efforts, including reauthorizing the Public Interest Declassification Board (PIDB) and (2) new bipartisan legislation was introduced in the U.S. Senate that focused specifically on modernizing the CNSI system, with a well-attended public committee hearing held on it.
- In May 2020, the PIDB published recommendations to support the vision for a uniform, integrated, and modernized security classification system that defends national security interests, instills confidence in the American people, and maintains sustainability in what is increasingly becoming an all-digital environment.
- The U.S. Government must invest in and use advanced technologies to support the CNSI system, including for the declassification and the management of large amounts of classified digital data. The recently enacted American Recovery Act included $1 billion for the Technology Modernization Fund for use in solving urgent cross-government IT challenges. Modernizing the CNSI system is such a challenge.
- We completed our new questionnaire to collect more accurate and useful CNSI oversight data from agencies, and will begin using it in FY 2021.

NSC-led Review of CNSI National Policies

We believe that the NSC's Records Access and Information Security directorate must lead a comprehensive interagency process to review and modernize critical national security policies governing the CNSI system. These policies include E.O. 13526, which was last updated in 2009 and serves as the backbone of the executive branch's system for managing classified information, and E.O. 12829, as amended, which governs classified information handled by U.S. Government contractors, licensees, and grantees. E.O. 12829 has not been sufficiently modernized since it was signed in 1993.

There have been numerous operational changes since these orders were written. Some, such as access to classified information while teleworking, have been highlighted because of the ongoing COVID-19 pandemic, while others, such as the need to leverage advanced technologies to ensure the efficient and effective declassification of huge amounts of digital data, predate the pandemic. New requirements have also impacted agency operations, including OMB M-19-21, "Transition to Electronic Records", a joint memorandum by OMB and NARA mandating new requirements for federal agencies to manage digital data, as well as Presidential Records Act and Federal Records Act amendments that added new requirements for classified records and definitions for digital materials.

Additional policy areas of E.O.s 13526 and 12829, as amended, that are in need of modernization include the following: updating automatic declassification processes and requirements to better facilitate the declassification of records; prioritizing records of significant historical interest for declassification reviews; assessing the benefits of simplifying the system by moving from three levels to two levels of classification to align with secure systems; improving and clarifying the use of classification challenges to ensure better classification decisions and increased transparency; reforming the

ISCAP to account for an increasing backlog of cases; and modernizing the NISP to account for uncleared contractors within the NISP supply chain. If the executive branch fails to modernize its CNSI policies, we believe that Congress will continue trying to satisfy these needs legislatively.

The NISP, established by E.O. 12829, as amended, still does not comprehensively address today's threats to classified systems and digital data operated and held by the NISP's government contractors, nor does it sufficiently cover the security vulnerabilities and exposures of uncleared contractors within the industrial supply chain. If this does not change, the United States will lose more and more of its most sensitive technology to those countries and bad actors who want to steal it.

Congressional Initiatives to Modernize the CNSI System

Two congressional initiatives significantly impacted the CNSI system in FY 2020.

First, the FY 2020 NDAA included numerous provisions that are designed to aid the modernization of the executive branch's CNSI system and support new national security imperatives. We believe five NDAA provisions will have an especially significant impact on these ongoing modernization efforts:

- (1) Reauthorizing the PIDB and establishing it as a permanent independent board dedicated to improving declassification work;
- (2) Requiring reports from each Intelligence Community Inspector General on the accuracy of classification decisions, proper marking, compliance with declassification requirements, and identifying and prioritizing topics of public and historical interest for declassification;
- (3) Mandating that the Department of Defense (DOD) reorient and align its Big Data policies with its cyber strategy, with a requirement to include classification standards and supporting metadata that better enable information sharing, collaboration, and use;
- (4) Directing reforms to how the Government conducts background investigations and adjudicates personnel security clearances, including requiring the Defense Counterintelligence and Security Agency to report on the backlog of personnel security clearances awaiting adjudication and a mitigation plan on how to reform processes; and
- (5) Including a Congressionally Directed Action requiring DOD to compile information about the declassification programs of all its components, including its plans to eliminate declassification backlogs and adopt the use of advanced technologies, such as Artificial Intelligence and Machine Learning, in declassification processes.

Secondly, the Declassification Reform Act of 2020 was introduced in the U.S. Senate, bipartisan legislation that focused specifically on CNSI declassification modernization efforts. The Senate Select Committee on Intelligence held a virtual public hearing on the proposed legislation on September 9, 2020. Discussion focused significantly on the PIDB's recommendation in its June 5, 2020 report to the President, *A Vision for the Digital Age: Modernization of the U.S. National Security Classification and Declassification System*, to designate the Office of the Director of National Intelligence (ODNI) as the Executive Agent for coordinating needed declassification reforms. Although the legislation fell one vote short of passing at the committee-level, we assess that it may be enacted into law in the future.

Additionally, more recently, Senators Ron Wyden and Christopher Murphy introduced legislation, the Transparency in Classification Act of 2020, which would provide the ISCAP with additional responsibilities and permit more Congressional oversight.

Modernizing ISOO Oversight and Metrics for Analysis

In FY 2018, and continuing in FY 2019, we embarked on a multiyear effort to reform our data collections we use to oversee agency CNSI programs. We wanted to develop a more accurate and effective way to measure and assess the health of agency CNSI programs that was less onerous and based only on data that we believe is (1) valuable for oversight; (2) mandated to be collected; or (3) helpful to agencies to improve their own CNSI programs. We also sought to streamline previous CNSI reporting requirements to us by consolidating them into one collection request.

In FY 2020, we continued to work extensively with stakeholders and subject matter experts - including those from federal agencies and civil society groups - to move this reform effort forward and gather recommendations to identify data that is meaningful, accurate, and measurable. As a result, we successfully completed a new data questionnaire for agencies that we believe accomplishes these goals.

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 program operations. As agencies were still working to quickly adapt to this altered environment for their programs, we believed that the likelihood of receiving meaningful reporting data in FY 2020 was greatly diminished. As a result, we delayed the deployment of our new comprehensive CNSI data collection questionnaire until FY 2021.

After we consulted with agencies, we determined that it would be helpful to provide them with the new questionnaire as early as possible in the reporting period to provide them with ample time to prepare for the new questionnaire content and format. Agencies received the new questionnaire early in calendar year 2021, and we plan to issue a formal agency tasking to complete it later in FY 2021. We believe that our data reform efforts are critical to understanding what changes are necessary to transform and reform the classification and declassification system, enhance information sharing, measure costs, complement cybersecurity policies, and support 21st century national security missions and needs.

Executive Order 13526, "Classified National Security Information" Oversight

Key Actions and Judgments:

- The total number of Original Classification Authorities (OCAs) continued to decrease across the Government.
- We reviewed 70 agency security classification guides (SCG) to ensure that they complied with the requirements of E.O. 13526 and its implementing directive. While most of these SCGs met these requirements, approximately 20% of SCGs had multiple elements for which the security classification level was ambiguous, and 14% of SCGs had multiple elements for which the date or event for classification failed to comply.
- Approximately 25% of the SCGs listed a date they were issued or last reviewed that exceeds the five-year regulatory-mandated time frame for such updates.
- My office worked with the Department of State to contribute CNSI subject-matter expertise to ongoing bilateral information security consultations with the Government of Japan.

Original Classification Authority Designations

The total number of OCAs across the executive branch continued to fall in FY 2020. Agencies reported an overall reduction of 187 OCAs from FY 2019 to FY 2020, which represents a 10.9% decrease. The FY 2020 figures include 678 Top Secret level OCAs, 848 Secret level OCAs, and 3 Confidential level OCAs.

Security Classification Guide Assessments

In FY 2020, we began a multi-year review of agency SCGs to determine if they are prepared in accordance with the requirements of E.O. 13526 and 32 CFR Part 2001, and with sufficient specificity to facilitate proper and uniform derivative classification. Derivative classification is the incorporation, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. While derivative classification accounts for the vast majority of classification actions, the genesis of the classified information is in the determinations made by OCAs. SCGs are the primary means by which OCA decisions are recorded and communicated, and as such are a key component of the security classification system.

These assessments differ from the Fundamental Classification Guidance Review (FCGR), which agencies last completed in FY 2017. The FCGR requires agencies to complete a comprehensive review of their classification guidance to ensure that it reflects current circumstances and that it identifies classified information that no longer requires protection and can be declassified. Our SCG review examined the content of a sample of the agencies' guides to determine if they meet the requirements of E.O. 13526. Our goal is to review samples of SCGs from every agency that produces them.

Our SCG review evaluates how fully the agencies' SCGs are complying with the administrative and technical requirements of E.O 13526 and 32 CFR Part 2001. The administrative requirements specify that the SCG must be approved personally and in writing by an official with program or supervisory responsibility over the information or is the senior agency official who is authorized to classify information originally at the highest level of classification prescribed in the SCG. This OCA must be identified in the guide by name and position, or by a personal identifier.

Other administrative requirements spell out that each SCG must identify its subject matter and identify an agency point of contact for any questions about the SCG. It must also provide the date the SCG was issued or when it was last reviewed. Each SCG must have been reviewed and updated as circumstances require, but at least in the past five years.

The technical requirements mandate that each SCG must state precisely the elements of information to be protected; it must indicate which classification level applies to each element of information, and, when useful, specify the elements of information that are unclassified; it must state a concise reason for classification which, at a minimum, cites the applicable classification category or categories in E.O. 13526, section 1.4; and it must prescribe a specific date or event for declassification or, if appropriate, one of the exemption codes specified in E.O 13526 and 32 CFR Part 2001.

Through the end of FY 2020, we reviewed 70 SCGs from multiple agencies and their subordinate components. For the most part, these SCGs generally met the requirements of E.O 13526 and 32 CFR Part 2001. We assessed that many of the SCGs were excellent, although it was rare both for an SCG to be perfect or chronically deficient. The subject matter contained within many of the reviewed SCGs is complex or highly technical in nature, and it was clear to us that many agencies had expended considerable effort in drafting them. A large number of agencies have issued SCG templates, which, when followed, help to ensure that all of the required SCG elements are included.

Most of the deficiencies we identified were minor and limited in nature, though some contained multiple omissions or significant deficiencies in meeting individual requirements. All the SCGs included the date they were issued or last reviewed, and all but a handful identified their subject matter and a point of contact for questions about the SCG. Nearly one fifth of the SCGs failed to provide sufficient information to identify the OCA, and in several others, the individual who signed the SCG is not on the agency OCA list, which is prohibited. Nearly one quarter of the SCGs we examined list a date they were issued or were last reviewed that exceeds the five-year timeframe. In a few instances, we found that some agencies had not reviewed between one-third and one-half of their SCGs in over five years.

Turning to the technical requirements, we observed that the vast majority of the SCGs precisely state the elements of information that must be protected. However, more than one in five of the SCGs had multiple elements for which the classification level was ambiguous. For example, an SCG might indicate a range of classification levels that apply to a particular element of information, but does not indicate what conditions would require it to be classified at one level as opposed to another.

The OCA must specify this information in the SCG and not leave it to the derivative classifier to determine. About one in seven of the SCGs failed to spell out the reason for classification, either by not providing a reason for multiple elements or by not giving a reason for any of them. About one in seven of the SCGs had multiple elements for which the date or event for classification was missing or was not in accordance with E.O. 13526 and 32 CFR Part 2001.

Of most concern in this area were ten SCGs that instructed the users to apply one or more of the 25X1 through 25X9 exemptions, which exempt information from automatic declassification at 25 years and allow for classification up to 50 years. Agencies must receive approval from the ISCAP to apply these exemptions. Although the ISCAP has given a few agencies the authority to use these exemptions at the time of automatic declassification (at 25 years), it has very rarely extended that authority at the time of the document's origin. The two agencies that prepared these ten SCGs did not have the authority to use these exemptions in their SCGs.

SCGs are essential to the proper functioning of the classification system. They communicate the OCA's decisions, which are necessary to facilitate effective and uniform derivative classification of information, which notably makes up most classification decisions. As such, it is critical that SCGs are accurate and provide, at a minimum, the information required by E.O. 13526 and 32 CFR Part 2001 with sufficient detail and precision.

Many of the SCGs do this very well and demonstrate a continuing commitment to excellence. Nevertheless, some fall short, and their creators need to be more careful in ensuring that their SCGs provide the required information. The ISOO SCG review will continue in FY 2021. Agencies should take our findings to heart and review and revise their SCGs as needed to ensure that they are accurate, precise, up-to-date, and prepared in accordance with the requirements of E.O. 13526 and 32 CFR Part 2001, and that they provide clear guidance to the derivative classifier.

Special Access Program (SAP) Assessments

We began reviewing agency SAP programs in FY 2019, focusing on whether agencies were complying with the requirements of E.O. 13526 and 32 CFR Part 2001. Our methodology for this examination includes a review of agency policies, procedures, and processes governing SAP establishment, implementation, management, and internal oversight. We continued our reviews in early FY 2020, but we had to suspend them because of COVID-19 pandemic restrictions. We will restart our reviews after we and the subject agencies return to normal operations. SAP information is among the most sensitive classified information that the U.S. Government generates; it is essential that agencies manage their SAP programs effectively and by following established policies.

Bilateral Information Security Consultations with the Government of Japan

My staff, working with the Department of State, provided its CNSI subject-matter expertise to ongoing bilateral information security consultations (BISC) with the Government of Japan. These consultations are part of larger U.S.-Japan Alliance efforts to advance this important bilateral relationship, which serves as a cornerstone of peace, security, and prosperity in the Indo-Pacific region and around the world. Differences in our information security are roadblocks to sharing the critical information to achieve the next level of Alliance relationship we need. The United States views the BISC as a foundational, whole-of-government initiative, critical to enhancing our ability to share defense- and security-related information across the spectrum of our common military, economic, and diplomatic priorities.

Executive Order 12829, "National Industrial Security Program" Oversight

Key Actions and Judgments:

- The National Industrial Security Program Operating Manual (NISPOM) updates are expected to be completed in FY 2021, although the process to update it remains slow and is neither flexible nor agile enough to meet the national security threats it is supposed to address.
- We saw continued and substantial progress in reducing security clearance backlogs and modernizing vetting processes, making certain that employees are able to start working sooner and mitigating potential threats posed by insiders more quickly.
- We led discussions aimed at waiving National Interest Determinations (NIDs) for U.S. companies if they meet several requirements spelled out in Section 842 of the FY 2019 NDAA, which became fully operational for all Cognizant Security Authorities (CSAs) on October 1, 2020. This resulted in the more efficient use of resources in overseeing contractors that are owned or controlled by certain non-U.S. citizens or foreign entities.
- We coordinated and led interagency meetings on reforming NISP cost calculation methods. These meetings were focused on improving processes and ensuring that we collected more precise data for both agency and industry costs on how much they spend to implement the NISP.
- We observed a considerable increase in communications between industry and the ODNI, as the Security Executive Agent, and the Director of the Office of Personnel Management (OPM), as the Suitability and Credentialing Agent, along with the Performance Accountability Council, that reflects continued transparency surrounding the Trusted Workforce 2.0 efforts.
- The DOD is in the process of promulgating the NISP Contracts Classification System (NCCS) by means of a Federal Acquisition Regulation (FAR), which we believe will improve consistency and accuracy of security classification guidance provided to NISP contractors.

We are responsible for implementing and monitoring the NISP, pursuant to E.O. 12829, as amended.

We expect that a multi-year effort to update the NISPOM, led by the DOD, will be completed in FY 2021. DOD has submitted the proposed NISPOM federal rule for publication to OMB and to the Federal Register, for incorporation into the Code of Federal Regulations at 32 CFR Part 117. Contractors will have six months to comply with the rule from its effective date of February 24, 2021. The NISP CSAs will provide CSA mission-specific guidance to contractors under their security cognizance in accordance with executive branch coordination requirements before any such guidance is published. We believe that efforts to modernize E.O. 12829, its implementing regulation, and the NISPOM would be greatly enhanced by the simultaneous and coordinated modernization of E.O. 13526 and the CNSI program.

The ODNI, as the Security Executive Agent; the Director of OPM, as the Suitability and Credentialing Agent; and the Performance Accountability Council, continue to work toward greater transparency within the Trusted Workforce 2.0 efforts to modernize personnel vetting and security clearance reform. Communications have been strengthened among all parties by using industry fora, including the National Industrial Security Program Policy Advisory Committee (NISPPAC), National Defense Industrial Association/Aerospace Industries Association, Industrial Security Working Group, and Intelligence and National Security Alliance. These meetings have improved outreach as well as enhanced and facilitated communications about the NISP's security policies and practices.

The NISPPAC and its working groups have held numerous meetings to discuss and recommend updates to policies and instructions that promote cost savings and ways to mitigate threats and identify potential vulnerabilities to classified programs.

Following a multi-year development effort, the NCCS FAR now requires use of the DD Form 254 by both DOD components and non-DOD agencies that have industrial security services agreements with DOD, as well as use of the NCCS module of the Procurement Integrated Enterprise Environment, unless the non-DOD agency has an existing DD Form 254 information system. We commend DOD for the NCCS module, as it provides a uniform process for NISP classification guidance in a more timely, uniform, systematic, and automated way.

We will continue to engage both government and industry stakeholders to solicit their ideas for modernizing security policies, practices, and procedures.

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

Key Actions and Judgments:

- U.S. adversaries are aggressively targeting our sensitive unclassified information, systems, and other assets, damaging our economy and threatening our national security. The implementation of the CUI program is a critical component to combating these threats.
- We issued CUI Notice 2020-01, "CUI Program Implementation Deadlines", after consultation with the CUI Advisory Council and with approval from OMB. This Notice requires that any agency unable to meet the deadlines for various key CUI program requirements must submit an explanation and implementation plan or strategy outlining the cause for the delay and steps that will be taken to become compliant. We will review these responses and plans for approval or send them back for further coordination. Our goal is to ensure the timely and effective implementation of the CUI program across the executive branch.
- While there has been significant progress, the challenges of implementation continue to underscore the CUI program's breadth and the complexity of the underlying laws, regulations, and Government-wide policies that undergird the program and that have evolved over decades to safeguard and share unclassified information.
- We assess that the vast majority of executive branch agencies have made great strides in implementing the CUI program. Nevertheless, one large agency – the ODNI – is lagging far behind the rest. The ODNI's delays have emerged as an obstacle to the CUI program's implementation across the Intelligence Community. For example, intelligence agencies and components have indicated they face challenges as they begin integrating CUI markings and CNSI markings in co-mingled environments because of the need to move from existing practices to CUI's new marking conventions. These issues require the ODNI's leadership, working closely with us, to be solved. (See Table on page 17 for an agency-by-agency report on the status of what cabinet-level agencies and agencies on the CUI Advisory Council report as their timeline to issue agency CUI policy.)
- My staff has identified several areas for improving the program's implementation. The CUI Registry, established before the CUI implementing regulation at 32 CFR Part 2002 was published and shortly after E.O. 13556 was issued, was always intended to be a living, evolving compendium and is ripe for modernization. Updating the CUI Registry is currently underway, to streamline CUI categories, and provide clearer guidance that addresses what is covered by the CUI categories and their authorities.
- Full implementation will require additional resources, including dedicated funds and more full-time staff.

CUI Program Management 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. It designated NARA as the Executive Agent for the program, with NARA executing its responsibilities through the Director of ISOO.

As U.S. adversaries continue to target our sensitive, unclassified information and systems, the U.S. Government must adapt to counter these ever-growing threats. The CUI program, established to improve interagency information sharing while establishing consistent, standardized safeguards in the years following the 9/11 attacks, is a critical piece of the U.S. Government's response to these threats.

Approximately two-thirds of reporting federal agencies, including the DOD and a number of other large cabinet-level agencies, indicated in their annual report to ISOO that they have published, or were scheduled to publish, their agency's CUI policy by the December 31, 2020 deadline. Over 90% of agencies reported that they will have completed their agency's CUI policy by the end of calendar year 2021. The creation and issuance of CUI policy at agencies has proven to be one of the most critical parts of implementation, delaying compliance with other program elements until it is finished. Agencies generally report meeting the remaining elements of implementation within one year following the publication of their CUI policies.

Last year, agencies indicated challenges with disseminating CUI across the executive branch while maintaining the CUI program's safeguarding standards. In response, we formed an interagency working group that partnered with the National Information Exchange Model (NIEM) to release a Government-wide CUI metadata tagging standard reflected in NIEM Release 5.0 (**http://niem.github.io/niem-releases/**). ISOO will maintain this standard, with the support of the CUI Registry Committee, to ensure it stays up to date with any changes to the CUI program.

We believe that the full implementation of the CUI program at many agencies will continue to require additional resources. In FY 2016, ISOO worked with agencies and 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 inexcusably continue to impede implementation at those agencies that have failed to do so.

Continuing CUI implementation delays at the ODNI are adversely impacting the entire Intelligence Community as well as the rest of the executive branch. My office has received numerous reports from agencies that the ODNI's delays are hindering their own efforts to make progress towards fully implementing the program.

In December 2020, during the waning days of the last Administration and without any notice to us, the ODNI sent a letter to the National Security Advisor requesting that the President rescind E.O. 13556 and end the CUI program. We assess that this would have a devastating impact on the standardized sharing and protection of CUI across the federal enterprise, as well as with state, local, and tribal governments and private sector entities. Instead, the U.S. Government should accelerate its efforts to implement the CUI program. We must not return to the old, ad hoc "FOUO" (also commonly referred to as "SBU") system that was largely agency-specific, poorly integrated across the federal enterprise, and led to information sharing failures, including ones highlighted in the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) Report.

On March 24, 2021, I sent a letter to Director of National Intelligence Avril Haines expressing my concerns with the ODNI's CUI implementation efforts and offering to work together to enhance CUI program implementation at the ODNI. We look forward to working together with the new ODNI leadership to improve their compliance to levels commensurate with most of the rest of the government.

Federal Acquisition Regulation for CUI

We continue to wait for the General Services Administration (GSA) to publish the CUI Federal Acquisition Regulation (FAR) case, which was initiated in late 2016 and has been dormant at GSA since the fall of 2019. Once issued this regulation will standardize the way executive branch agencies require non-federal entities to comply with CUI safeguarding requirements. The Unified Agenda had projected that this FAR clause, a key part of agencies' CUI program implementation, would be released for public comment by March 2021 after a multi-year development process; however, this has not yet occurred and it is urgent that GSA prioritize its completion.

Agencies and contractors regularly contact us seeking its status and are actively awaiting the clause's publication. The lengthy delay in issuing the CUI clause is causing continued non-standardized approaches by agencies that disadvantage contractors and small businesses, and creating gaps in system and information security, as well as reporting.

Finalizing and issuing the CUI FAR remains a top priority of my office because it will significantly improve consistencies in government contracts that include CUI.

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 CNSI. It does not include or address current insider threat risks to CUI.

ISOO continues to believe that protecting CUI from insider threats is critical to the national interests and security of the United States. My office has worked with OMB and the ODNI's National Insider Threat Task Force on a draft policy solution to formally allow for, and to govern, the expansion of the National Insider Threat Program to include CUI and other unclassified critical systems and programs.

National Operations Security Program

ISOO worked with the NSC and federal agencies to ensure updates to the federal National Operations Security Program were sufficiently coordinated with CUI program requirements under E.O. 13556 so that both policies are consistent and appropriately integrated. The President signed National Security Presidential Memorandum (NSPM)-28, "The National Operations Security Program", on January 13, 2021, which modernized the executive branch's National Operations Security Program and replaced National Security Decision Directive 298 of January 22, 1988.

Department of Defense CUI Cybersecurity Initiative

The DOD's new Cybersecurity Maturity Model Certification (CMMC) initiative has the potential to aid CUI's implementation and improve cybersecurity for Defense Industrial Base (DIB) and DOD contractor systems. The CMMC combines cybersecurity controls 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 has outlined an interim certification process, and has begun designating the first members of a pilot group to test this process. We will continue to monitor its progress.

CUI Policy Completion by Cabinet and CUI Council Agencies

The CUI Executive Agent in consulation with the CUI Advisory Council developed deadlines for agencies to meet to achieve a phased implementation of the CUI program at the agency-level. These deadlines were issued in CUI Notice 2020-01. In that notice the deadline for agencies to issue their CUI policy was December 31, 2020. ISOO, recognizing the impact of the COVID-19 pandemic on agencies, provided a grace period of 6 month after the December 31, 2020 deadline. The third column denotes if an agency that missed the December 31, 2020 deadline reported that their program implementation was delayed by the COVID-19 pandemic.

Agency	Reported CUI Policy Status	Reported COVID-19 Delays
Central Intelligence Agency	2022 Dec 31	No
Department of Agriculture	2020 Dec	
Department of Commerce	Complete	
Department of Defense	Complete	
Department of Education	Complete	
Department of Energy	2020 Dec	
Department of Health and Human Services	2021 Jan	No
Department of Homeland Security	2021 Q1	No
Department of Housing and Urban Development	Complete	
Department of the Interior	Complete	
Department of Justice	2021 May 11	Yes
Department of Labor	Complete	
Department of State	2021 Oct	Yes
Department of Transportation	2020 Dec	
Department of the Treasury	Complete	
Department of Veterans Affairs	2021 CY	Yes
Environmental Protection Agency	2020 Dec 31	
General Services Administration	Complete	
National Aeronautics and Space Administration	2020 Dec	
National Science Foundation	2020 Oct	
Nuclear Regulatory Commission*	2022 Q2	No
Office of the Director of National Intelligence	2022 Dec 31	No
Office of Personnel Management	2020 Dec	
Small Business Administration	2021 May 31	No
Social Security Administration	Complete	
United States Agency for International Development	2021 Jun	Yes

*Note: NRC has submitted a draft policy to the CUI EA and is now on track to issue their policy in 2021

Color Key
Agency policy issued by November 1, 2020 when agency CUI Annual Report was due to ISOO
Agency projects their CUI policy to be issued by December 31, 2020 due date in CUI Notice 2020-01
Agency projects their CUI policy to be issued within calendar year 2021
Agency projects their CUI policy to be issued after calendar year 2021

ISOO Support for the Interagency Security Classification Appeals Panel

I serve as the Executive Secretary of the Interagency Security Classification Appeals Panel (ISCAP) in accordance with E.O. 13526, and my staff provides it with program and administrative support.

Key Actions and Judgments:

- The sizable ISCAP backlog of unresolved appeals is largely the result of a small number of requesters appealing large numbers of requests that Federal agencies were unable to decide upon within one year.
- The ISCAP should revise its criteria for the acceptance of appeals to (1) make them more equitable for greater numbers of ISCAP appellants to have their cases heard; (2) focus on more targeted appeals and historically significant declassification decisions; and (3) prioritize the most complex classification decisions.
- The ISCAP should transition from being a declassification "shop" of last resort for all appeals, to an appellate body with discretionary authority to determine which cases it will hear.

ISCAP Mandatory Declassification Review Appeals, Declassification Guide Review, and Appeals Case Backlog

The ISCAP decided two mandatory declassification review appeals and approved revisions to one declassification guide in FY 2020. It received 45 new appeals, increasing the backlog of unresolved appeals to 1,313 appeals. The ISCAP also administratively closed 16 appeals, including one classification challenge it received, either because the appeal did not meet the requirements for acceptance established by executive order or federal regulation, or because the appellant withdrew the appeal.

ISOO Support for the Public Interest Declassification Board

I also serve as the Executive Secretary of the Public Interest Declassification Board (PIDB) in accordance with P.L. 106-507, "The Public Interest Declassification Act of 2000, as amended" (the Act), and my staff provides the board with program and administrative support. Established by statute, the PIDB advises the President on issues pertaining to national classification and declassification policy.

Key Actions and Judgments:

- The PIDB published its report to the President in May 2020, providing a roadmap and specific recommendations on how to modernize the classification and declassification system.
- The COVID-19 pandemic significantly impacted the classification and declassification programs of executive branch agencies. These agencies will need to develop and implement modernized processes and take a risk management approach to address increasing backlogs and working with a decentralized or remote workforce.
- The COVID-19 pandemic has also brought to the forefront the need for a strong classified communication system that includes all equity holding agencies. Administration support and dedicated funds will be needed to fully implement this system.
- The COVID-19 pandemic limited the PIDB's ability to meet with stakeholders. It instead relied on virtual meetings and teleconference calls to publicize and socialize its report.
- Despite the COVID-19 pandemic, there was sustained interest in the PIDB's report recommendations, including in a congressional hearing and through proposed bipartisan legislation.
- The PIDB looks forward to working with the new administration on furthering their mutual goals for modernizing the classification and declassification system, and continuing its effort to advocate for increased transparency and public access to records of historical interest.
- There are currently two vacancies on the PIDB, one Presidential and one Congressional, to be filled.

Reauthorization of the PIDB

Although ISOO's support for the PIDB was suspended when the PIDB's statutory authorization lapsed on December 31, 2018, it quickly increased once the Congress reauthorized the PIDB on December 20, 2019.

PIDB Report and Recommendations

In May 2020, the PIDB published its report, *A Vision for the Digital Age: Modernization of the U.S. National Security Classification and Declassification System*, which was the culmination of four years of study and investigation. The report included recommendations on leveraging advanced technologies to improve classification and declassification, offered a roadmap for the executive branch on how to accomplish it, and assigned an Executive Agent to lead the reform.

In June 2020, the PIDB hosted a virtual public meeting with a wide variety of stakeholders to publicize its report and detail its recommendations.

In September 2020, PIDB member John Tierney testified virtually before the Senate Select Committee on Intelligence about the report and proposed reforms to declassification in S. 3733, The Declassification Reform Act of 2020.

PIDB Appointments

In June 2020, the terms of James E. Baker and Trevor W. Morrison, both Presidential appointees to the PIDB, ended. House Speaker Nancy Pelosi reappointed John Tierney to a second term on the PIDB in July 2020, and House Minority Leader Kevin McCarthy appointed Trey Gowdy to the PIDB in August 2020. Appointed by the Senate Majority Leader, Ken Wainstein's second term lapsed in September 2020, leaving the PIDB with only three members at the end of FY 2020. President Trump appointed four new members to the PIDB, Michael Lawrence, Benjamin Powell, Paul-Noel Chretien, and Ezra Cohen, in FY 2021. The President also made a fifth appointment, however, the appointee declined the nomination leaving one Presidential vacancy, as well as one Congressional vacancy for the Senate Majority Leader's appointment.

Congressional Request to Review Classified Records

The PIDB received and accepted a congressional request from Senator Christopher Murphy in September 2020 to review five 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, its review of the records has been delayed due to the COVID-19 pandemic, secure facility closures, the requirement for new board members to obtain all appropriate security clearances, and legal requirements in the Presidential Records Act.

PIDB Outreach

In FY 2020, the PIDB published 23 posts on its blog, *Transforming Classification*, contributing to a robust dialogue in the areas of classification and declassification. Many posts supported recommendations contained in the PIDB's report, while others provided information on related areas of interest.