2020

A Vision *for the* Digital Age: Modernization *of the* U.S. National Security Classification *and* Declassification System

RECOMMENDATIONS SUBMITTED by the
PUBLIC INTEREST DECLASSIFICATION BOARD
MAY 2020

Table of Contents

May 26, 2020

The Honorable Donald J. Trump
President of the United States
The White House
Washington, DC 20500

Dear Mr. President:

The FY 2020 National Defense Authorization Act that you signed into law on December 20, 2019, included a provision reauthorizing the Public Interest Declassification Board. With this reauthorization, the members of our Board continue to advocate for modernizing classification and declassification policies and processes as a means of cutting costs, improving agency digital business practices, combating over-classification, improving declassification, and establishing a transformed, credible security classification system.

Today, in this report, we offer recommendations that strongly support your directives and policies to modernize Government Information Technology (IT) by laying out our vision for a future system of classification and declassification that will operate effectively and efficiently in the digital environment. We build upon our previous work by offering new recommendations for how to achieve these goals.

Transformation will be difficult. When it comes to declassification, the Government is still in the analog age. The current system was created before the United States entered World War II, and it remains entrenched today. Despite rapid increases in the volume and variety of digital data, the Government still relies upon inefficient and ineffective paper-based processes. The momentous change that is required cannot be achieved without Presidential leadership to drive reform. As a part of this report and set of recommendations, we propose that you designate a cabinet-level Executive Agent responsible for designing and implementing a new security classification system for the digital age. We further recommend that the Executive Agent, working with an Executive Committee, should have authority to implement changes across agencies and at the enterprise level. The longer the Government waits before adopting new technology in this area, the exponentially further behind it will be in making much needed reforms.

The PIDB stands ready to answer any questions you or members of the Executive branch may have about our report. We also are eager to help improve policies governing classified national security information, aid our national security, enhance transparency, and support the Government's IT modernization efforts across the Executive branch. Thank you.

Sincerely,

Trevor W. Morrison
Chair, 2016–2018

James E. Baker
Acting Chair, 2018, 2019–2020

A Vision for the Digital Age

PIDB VISION FOR THE FUTURE

Our vision is a uniform, integrated, and modernized security classification system that protects national security interests and instills confidence in the American people and is also sustainable in the digital environment. The declassification business model that we envision for the future centers on (1) organizing for success via a more unified and federated enterprise-level, system-of-systems approach to declassification; and (2) acquiring and adopting technologies and processes that leverage cutting-edge IT, telecommunications innovation, and systems development.

STRATEGIC POLICY CHANGE: HOW TO DO IT

The PIDB developed specific Concepts and Recommendations for modernizing the declassification of Federal Government records going forward.

1. Designate an Executive Agent (EA) and Executive Committee with authorities and responsibilities for designing and implementing a transformed security classification system.
2. Organize the national security declassification community into a federated National Declassification System (NDS). Operate the NDS in a system-of-systems enterprise to streamline and modernize classification and declassification policies, processes, and technologies.
3. Empower the National Declassification Center (NDC) with the authorities and responsibilities to oversee the implementation of the NDS system-of-systems enterprise approach for managing classified information across the Executive branch, and working with the originating and equity-owning agencies.

STRATEGIC TECHNOLOGY CHANGE: HOW TO DO IT

1. Transition to using technology, including tools and services for managing Big Data, Artificial Intelligence, Machine Learning, and Cloud storage and retrieval, to produce systems and services which support automated classification and declassification. This transition should institutionalize research and development activities across Government, incentivize private industry participation in these areas, and reform technology acquisition.

IMMEDIATE IMPACT: NEAR-TERM IMPROVEMENTS

1. Direct the Secretary of Defense, the Director of National Intelligence, and the Secretary of Energy to develop a unified or joint plan and to assist the Archivist of the United States in modernizing the systems in use across agencies for the management of classified records, including electronic records.
2. Deploy technology to support classification and declassification automation.
3. Implement secure information technology connectivity between and among all agencies managing classified information, specifically including the National Archives and Records Administration (NARA), which manages the NDC and classified records of the Presidential Libraries.
4. Empower the NDC to design and implement a process to solicit, evaluate, prioritize and sponsor topics for declassification Government-wide, in consultation with the public and Government agencies.
5. Develop a new model for accurately measuring security classification activities across Government, including all costs associated with classification and declassification.
6. Simplify and streamline the classification system; decide how to adopt a two-tiered classification system.

PIDB

WHY THE PIDB DID THIS STUDY

There is widespread, bipartisan recognition that the Government classifies too much information and keeps it classified for too long, all at an exorbitant and unacceptable cost to taxpayers. Despite the Government's significant financial investment in the security classification system, over-classification continues to impede the appropriate sharing of information. Inadequate declassification contributes to an overall lack of transparency and diminished confidence in the entire security classification system. This trend may encourage dangerous information leaks from within Government.

The time is ripe for envisioning a new approach to classification and declassification, before the accelerating influx of classified electronic information across the Government becomes completely unmanageable. The status quo for classification and declassification is ineffective and will not work in the digital age. The Government needs a paradigm shift, one centered on the adoption of technologies and policies to support an enterprise-level, system-of-systems approach.

The Public Interest Declassification Board (the PIDB) continues to advocate for the modernization of classification and declassification policies and processes across Government as a means of combating over-classification, improving declassification, and ensuring a credible security classification system.

To aid this effort, the PIDB presents this vision for the future security classification system.

Executive Summary

There is widespread, bipartisan recognition that the Government classifies too much information for too long, at great and unnecessary cost to taxpayers. This problem is getting worse, as the volume of classified information grows at an increasing rate. Current policies, practices, and technologies for managing classified information must be modernized for the digital age.

The time is ripe for envisioning a new approach to classification and declassification, before the accelerating influx of classified electronic information across the Government becomes completely unmanageable. The status quo for classification and declassification can no longer function without a paradigm shift focused on the adoption of technologies required to implement an enterprise-level, system-of-systems for Government information management.

The Public Interest Declassification Board (PIDB) offers this vision statement, developed to aid in constructing the integrated security classification system so urgently needed today:

A Vision for the Future of Classification and Declassification

Our vision projects a uniform, integrated, and modernized security classification system that appropriately defends national security interests, instills confidence in the American people, and maintains sustainability in the digital environment. The declassification business model that we envision for the future centers on: (1) organizing for success via a more unified and federated enterprise-level, system-of-systems approach to declassification; and (2) acquiring and adopting technologies and processes that leverage cutting-edge IT, telecommunications innovation, and systems development.

Strategic Policy Change: How To Do It

1. Designate an Executive Agent (EA) and Executive Committee with authorities and responsibilities for designing and implementing a transformed security classification system.

   The EA should develop a long-term strategy for the sustainability of Government-wide reform efforts, potentially assigning authorities and responsibilities to an Executive Committee. The best initial choice is the Director of National Intelligence (DNI). As the leader in the successful implementation of the Intelligence Community Information Technology Enterprise (ICITE), the Office of the Director for National Intelligence (ODNI) has the expertise and experience to design and implement a transformed security classification system. In fulfilling this role, the DNI should work closely with White House innovation and IT initiatives and with the Office of Management and Budget (OMB). OMB is accountable to the President and the Congress, already manages interagency processes, and understands and holds a stake in identifying costs and savings associated with executive-branch programs. The Committee should be made up of appropriate senior leaders at departments and agencies with significant equities in this area—especially the offices of the Director of National Intelligence, the Under Secretary of Defense for Intelligence, the Secretary of Energy, and the Archivist of the United States—and chaired by the DNI.

2. Organize the national security declassification community into a federated National Declassification System (NDS), operating as a system-of-systems enterprise to streamline and modernize classification and declassification policies, processes, and technologies.

   Programmatic and technical requirements will provide a risk-based, output-oriented architecture supporting timely public access to historically significant and permanently valuable information that will aid end-users, especially policymakers and historians.

3. Empower the National Declassification Center (NDC) with the authorities and responsibilities to oversee the implementation of the NDS system-of-systems enterprise collective approach for managing classified information across the Executive branch, working with the originating agencies.

   Only with adequate resources and with strict implementation deadlines and mandates for managing collective resources to support shared outcomes can the NDC achieve the potential for improvement. The NDC requires authorities to act, sanction, and fund the NDS. It must have oversight, tracking, and coordination responsibilities for the NDS, operating with records holders as a federated and cooperative collective. Leadership at the NDC should have sufficient interagency experience and qualifications, including the ability to perform Federal acquisition functions that underpin research and development of the new technologies and architectures necessary to achieve the long-term potential of a cost effec-

tive NDS. Management must coordinate the NDC authorities and the NDS collective, while remaining mindful of Federal department and agency equities.

Strategic Technology Change: How To Do It

1. Transition to using technology, including tools and services for managing Big Data, Artificial Intelligence, Machine Learning, and Cloud storage and retrieval, to produce systems and services that support automated classification and declassification. This transition should institutionalize research and development activities across Government, incentivize private industry participation in these areas, and reform technology acquisition.

   Capitalize on the current IT success of emerging and existing information technologies and communications to galvanize the modernization of the classification and declassification system. The President's Management Agenda[1] promotes and is poised to drive a modernized, multi-generational IT infrastructure change across the Government. These aligned efforts must bridge public-private industry opportunities and work across agencies in coordination with stakeholders, including allies.

The Importance of Making These Choices: Systemic Issues Impeding Transformation

1. Outdated and excessively costly, the current method for classifying and declassifying national security information remains unsustainable in the digital information age. As all media become fully digital, analog technology and paper records become practically inaccessible and dysfunctional.
2. The costs of the security classification system are staggering (reported to be an estimated $18.39 *billion* in FY 2017), yet resources for declassification remain woefully underfunded, while over-classification and the declassification backlog give rise to leaks and inadvertent disclosures that damage national security imperatives.[2]
3. By continuing to unnecessarily classify and over-classify information without timely declassification and strategic transformation of the information system, the volume and diversity of records inaccessible to policymakers and the public will only continue to increase.
4. Current practices diminish public confidence in the security classification system, impede appropriate information-sharing within the Government, and reduce the open discussion of our national history that is so critical to the democratic process. The Government struggles to increase transparency and to demystify its classified activities.
5. Outdated technology, insufficient staffing, and a limited budget undermine the mission of the NDC and the National Archives and Records Administration (NARA), which need an influx of resources to improve their capabilities.

Our vision for the future state of classification and declassification calls for a sustainable security classification system transformed to operate in a fully digital information environment. It will support and enhance the classification and declassification of all government information, especially the records most relevant to historians, researchers, and policymakers. A system-of-systems design will support this modernized architecture by pooling resources, talent and capabilities to support a more complex organization capable of providing improved functionality and performance in classification and declassification across agencies.

6. At present, NARA simply cannot manage any volume of classified electronic records, while its ability to manage unclassified electronic records remains severely limited by inadequate resources. In the very near future, the current lack of basic resources will prevent NARA from storing and managing all formats of classified and unclassified records, whether analog or digital. Without immediate action, NARA's ability to implement its mission remains unlikely to improve in the near-term.

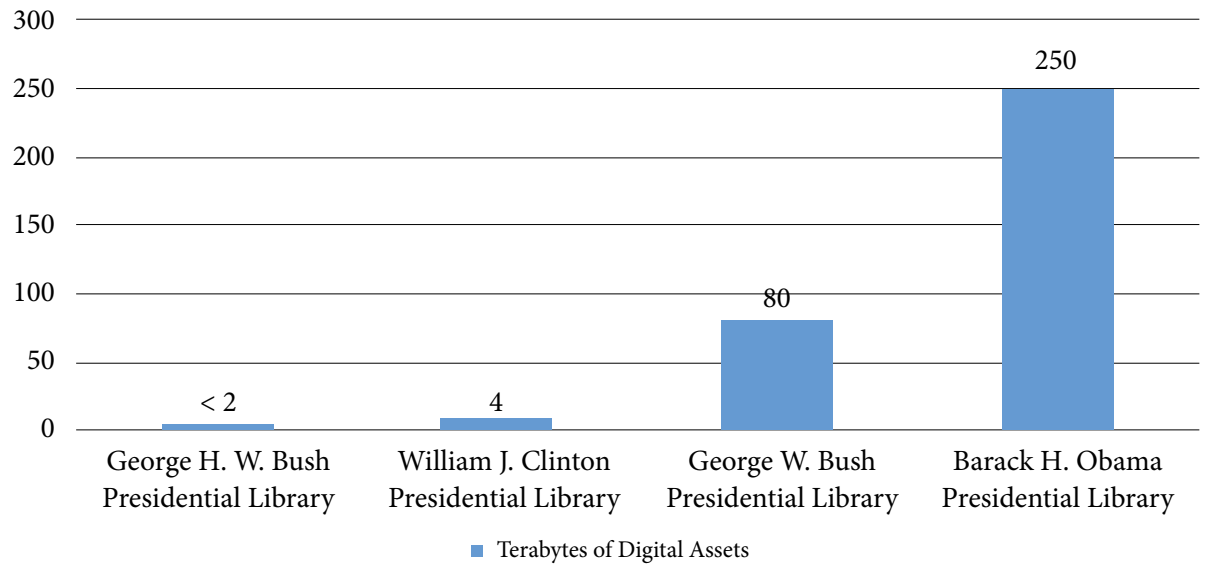
Immediate Impact: Near-Term Improvements

The systemic change we envision and advocate is vitally and urgently important. It will also require substantial commitment and effort at a Government-wide level. (See Figure 1 for an example showing the dramatic growth in digital assets created in recent Presidential administrations now stored at NARA). While pursuing that change, however, we also identify a number of immediately feasible improvements to the current system that could be made now:

1. Direct the Secretary of Defense, the Director of National Intelligence, and the Secretary of Energy to assist the Archivist of the United States in modernizing the systems used across agencies for the management of classified records, including electronic records.
2. Deploy technology to support classification and declassification automation.
3. Implement secure information technology connectivity between and among all agencies managing classified information, specifically including NARA, which manages the NDC and the classified records of the Presidential Libraries.
4. Direct the NDC to design and implement a process to solicit, evaluate, prioritize, and sponsor topics for declassification across the Government, in dialog with Government agencies and the public.
5. Develop a new model for accurately measuring security classification activities across Government, including all costs associated with classification and declassification.
6. Simplify and streamline the classification system; decide how to adopt a two-tiered classification system.

Figure 1

Increase in Digital Assets
Within Presidential Libraries
National Archives and Records Administration
1989–2017



The rapidly expanding volume of electronic records accessioned by each new Presidential Library, compounded by a growing variety of digital assets, challenge the legacy systems that still process Federal records. While digital collections at the George H. W. Bush and William J. Clinton Presidential Libraries mainly include email records, the Presidential Libraries of George W. Bush and Barack Obama maintain a complex array of digital assets that range from email to a variety of datasets, websites, videos, and social media. Analog formats and unstructured data embedded in the archival accessions further underscore the need for Government-wide innovation and modernization in classification and declassification.

A Vision of the Future State of Classification and Declassification

Background: Challenges in the Current Paradigm

Classification and declassification policies and processes have not kept pace with the rapid explosion of data in the digital information age. As the volume of digital information that the Government must manage grows exponentially, agencies remain unable to adequately manage and exploit today's Big Data resources, let alone prepare for the tsunami of digital information anticipated in the years ahead. For an example of how this digital explosion affects the Presidential Libraries within the National Archives and Records Administration (NARA), see Figure 1 on the preceeding page. The Internet revolution, the transition to email and other forms of instantaneous communications, and the pervasive use of social media applications have profoundly altered the way the Government conducts business, and how agencies perform their missions, while producing unprecedented volumes of data in need of appropriate organization, management and control.[3] As a result, the unmet, Government-wide need to manage proliferating volumes of sensitive and classified digital information in a sound and consistent manner raises serious concerns.

Currently, management of classified information largely follows established analog and paper-based models long in place at agencies. Executive branch classification, declassification, and records management functions have fallen dramatically behind in anticipating and preparing for the current influx of digital information. The failure to modernize information access—both for the public and for officials inside the Government—incurs significant financial costs. It also undermines public confidence in the credibility and competence of Government officials and Federal institutions. The security classification system itself imposes much of these costs.

The expectation of more efficient access by users of Government information and the normalization of an open information environment in society at large increases the need to protect Government secrets vital to national security and those secrets alone. To provide the appropriate and necessary access to, and safeguarding of, Government information, agencies must modernize information governance, transforming classification and declassification so that the Government functions effectively and efficiently in the digital information environment, while preparing to better manage classified information in the future.

Assumptions, Principles, and Drivers for a Future Vision

The digital environment inherently links information management functions, including classification, declassification, records management, and information security. Only cooperative and complementary reform efforts can modernize these linked but outmoded Government functions. The strategic principles of reducing over-classification, improving declassification, and ensuring a credible security classification system must guide this programmatic transformation.

Information management faces major resource constraints, especially in declassification. Considering its Government-wide mandate, the lack of adequate funding and technology for the National Declassification Center (NDC), located within the NARA, is particularly noteworthy. Without significant resource investment in the NDC, responsibility for managing declassification and handling classified information falls to individual departments and agencies, and to NARA, all of which lack sufficient funding and technology for these critically important processes.

Although individually responsible for managing classified information, each agency needs to apply a new set of governance and organizing principles to amend and strengthen relationships between their organizations in order to support a Government-wide, system-level approach to declassification. The government as a whole needs to design and implement a more integrated, federated, and centralized system that adopts a virtual and community-centered method of declassification with technology at its core.

A modernized declassification system must ultimately account for the functions critical to end-users—both public and Government—including policymakers and historians. Fundamentally, the system must be able to search, retrieve, and use previously declassified archival data. Due to NARA's resource constraints and its slow progress in managing electronic records, in some cases, a modernized system must shift the preservation of declassified information from NARA to the originating departments and agencies. Without the funding needed to develop expertise and a technical alternative,

Previous PIDB recommendations called for an examination of technology solutions to aid classification and declassification, both by automating current workflow processes and by assisting decision-making. We have previously noted the successful development of a decision-support technology created at the request of the CIA and NARA at the Center for Content Understanding (CCU) at the Applied Research Laboratories at the University of Texas at Austin. At the CCU, scientists examined the ability to achieve machine-assisted sensitive content identification in classified records and developed the Sensitive Content Identification and Marking (SCIM) tool. The pilot examined 87,000 email records from the Reagan Administration using a combination of Natural Language Processing, expert systems, Machine Learning, and semantic knowledge representation to identify sensitive content. The PIDB's June 2015 public meeting featured experts who developed the SCIM tool and noted the pilot demonstrated substantially accurate identification of classified information.

continued on next page.

NARA is unlikely to provide the large automated system required to manage the volumes of classified data currently generated (and ever greater volumes expected in the future).

In the interests of simplification and standardization, the Records Access and Information Security Policy Coordinating Committee (RAIS PCC) chaired by the National Security Council (NSC) should decide how to adopt a two-tiered classification system as the United Kingdom and other allies have done. When adopted, this change would reflect the de facto state of classification in the digital environment, where information resides in systems on either a SECRET or TOP SECRET level. Appropriate controls and handling categories, as well as the implementation of the Government-wide Controlled Unclassified Information (CUI) program, will remain part of the system.

Vision Statement: a Long-Term Illustration of the Future System

A sustainable security classification system transformed to operate in a fully digital environment will support and enhance the correct classification and declassification of information in all forms, and identify information of historical and public policy interest. A system-of-systems design and architecture will support the modernized system, pooling resources and capabilities to deliver a structure capable of providing improved functionality and performance in classification and declassification across agencies.[4] System-of-systems engineering will enhance classification and declassification by developing processes, tools, and methods for designing, re-designing, and deploying unique solutions to programmatic functions.[5] Wherever possible, the integral automation of processes will operate as the cornerstone of the new system design.

The adoption of a robust Risk Management Framework (RMF) is key to the automation of processes across all agencies. The framework must be aligned to agreed-upon goals and objectives. Risk must be better identified, assessed, responded to, monitored, and reported at a system-wide level.[6] The current analog process of sequentially referring classified records to multiple agencies with equities under review must be minimized to the greatest extent possible.

The search for more sophisticated technology tools to assist classification and declassification decision-making continues. AI promises more accurate and timely classification and declassification if adopted as part of a Government-wide technology investment strategy. AI can build on the successes of the SCIM tool and improve information sharing, downgrading, redaction, and declassification actions. AI provides the most promising technological capability that can transform classification and declassification. Its potential reinforces the PIDB's call for agencies to develop technology pilot projects, institutionalize research and development activities, and reform acquisition practices to advance classification and declassification technology and architectures.

To see the in-depth CCU project briefing with visual subject matter given in June 2015, please see PIDB's meeting of June 25, 2015 and PIDB's blog *Transforming Classification*: https://transforming-classification.blogs.archives.gov/.

Some level of agreed-upon risk tolerance must allow the NDC and each agency to make limited declassification decisions concerning the equities of other agencies. Similarly, in classification, agencies need to consider risk tolerance when evaluating the implications that the classification of information has for information sharing and decontrol.

Real-time decision-making in classification and declassification will occur with the assistance of advanced technologies, which, in pilot tests and in current use,[7] conclusively demonstrate superior accuracy to human review. Content understanding, Machine Learning, Natural Language Processing, and other advanced technologies will assist in searches of sensitive and classified information. Artificial Intelligence (AI) and other Machine Learning technologies will play a significant role in amplifying and complementing nuanced human decision-making in classification and declassification, improving the accuracy and timeliness of access to classified records. [8]

The application of standards, rules, and guidance will be critical to the implementation and functionality of these technologies. NARA and the NDC will lead in establishing this governance with the assistance and input from key agencies, and by overseeing implementation rather than attempting to continue the current practice of employing declassification review at one physical location.

A universal "grand bargain" is necessary to define the changing roles of NARA, the NDC, and key agencies in assigning appropriate authorities and responsibilities within a modernized system. NARA will play a pivotal role in the new declassification process, perhaps even in supporting the acquisition and development of technology, as well as by serving as the primary center for processing classified records. NARA guidance and directives concerning records management, especially with regard to the requirements for universal electronic records management, will support the new declassification paradigm.

Setting priorities for declassification will begin to mitigate ongoing resource constraints and the backlog of records in need of review at agencies. To appropriately set priorities, the new system will implement better-defined rules for identifying "permanently valuable" classified records that warrant systematic declassification review, leaving the remainder for review only when requested by a researcher.

The PIDB's 2014 Report to the President, *Setting Priorities: An Essential Step in Transforming Declassification*, makes the case for the Government to adopt a centralized approach to topic-based prioritization and recommends specific policy and process changes aimed at improving access to historically significant records most sought-after by the public.

With input from the public, agency classifiers, declassifiers and historians, the recommendations found in this supplemental report are meant to assist the Records Access and Information Security Policy Coordination Committee (RAIS PCC) in developing a Government-wide approach to fundamentally transforming the security classification system.

The PIDB concluded that automatic declassification should no longer be the sole policy driving declassification programming across government. In practice, automatic declassification has fueled a risk-averse process that limits quality declassification review, generates expensive re-reviews, and adds unnecessary costs to an overburdened system. As the volume of information continues to increase exponentially, topic-based prioritization ensures declassification review of records with the greatest potential use by the public, historians, public policy professionals and the national security community. Prioritization will more closely align with electronic

continued on next page.

information management practices designed to ensure discovery and access to relevant information.

The *Setting Priorities* Report provided six recommendations in support of topic-based prioritization that gives greatest attention to records of public interest:

1. Topic-based declassification should be the normal process rather than the exception.
2. The NDC, in consultation with the public and with agencies, should design and implement a process to solicit, evaluate and prioritize standard topics for Government-wide declassification.
3. End pass/fail determinations and identify necessary redactions for topic-based reviews.
4. The Government should require agencies to develop and use new technologies to assist and improve declassification review.
5. Agencies and the NDC must improve risk management practices.
6. Revisions to the current Executive Order are needed to lessen the burden of automatic declassification on agencies in support of topic-based declassification review.

Setting Priorities also included a list of topics solicited from the stakeholders inside and outside Government. This list should provide a suitable starting point for Government policymakers to begin designing and implementing a prioritization process.

Crucial reforms to the system will include a tightening of definitions and greater specificity for categories requiring protection in the first place. Some measure of constraint on the system will be necessary to combat over-classification, a topic which requires broader study and more clearly defined outcomes to reverse the trend of excessive secrecy. Over-classification manifested in excessive secrecy is and will remain a serious challenge to appropriate information sharing and control. The benefits of sharing classified information with properly cleared users outweighs the perceived detriments of inappropriate distribution. Classification need no longer be the default selection to ensure national security interests are adequately protected. The future system will manage all classified information to include Restricted Data (RD) and Formerly Restricted Data (FRD) information and classified Congressional records.

Strategy to Achieve the Future Vision: Recommendations to Facilitate Strategic Policy Change

1. Designate an Executive Agent (EA) and Executive Committee with authorities and responsibilities for designing and implementing a transformed security classification system.

   The vision of a future security classification system transformed to operate in a fully digital information environment will require White House endorsement and leadership. The President will need to designate an EA responsible for designing and implementing the future paradigm. The EA will need to develop a long-term strategy for the sustainability of reform efforts, potentially realigning authorities and responsibilities for the program to an Executive Committee made up of appropriate senior leaders at those departments and agencies most impacted (i.e. Office of the Director of National Intelligence, Office of the Under Secretary of Defense for Intelligence, the Secretaries of State and Energy, and the Archivist of the United States) and led by the Director of National Intelligence.

   In the new paradigm, the EA will ensure a centralized yet federated Government-wide collective by redefining organizational and governance

processes to serve the equities of both NARA and classified information managers across the government. The EA will also give consideration to establishing an acquisition approach and contracting techniques in support of innovation and IT tool development.[9]

The best initial choice for the EA is the Director of National Intelligence. As the leader in the successful implementation of the Intelligence Community Information Technology Enterprise (ICITE), ODNI has the expertise and experience to design and implement a transformed security classification system. In fulfilling this role, the DNI should work closely with White House innovation and IT initiatives and with the Office of Management and Budget (OMB). OMB is accountable to the President and the Congress, already manages interagency processes, and understands and holds a stake in identifying costs and savings associated with Executive branch programs. [10]

Successful design and implementation of the future vision will require agency support, as well as public endorsement from leaders in the public interest groups and Sunshine in Government Community. The PIDB can serve as a conduit for public participation and can continue to advise the President and the leaders of Congress on the transformation of the security classification system.

2. Deploy technology to support classification and declassification automation.

Only strict implementation deadlines and mandates for increasing resources in support of shared outcomes can achieve the necessary improvement. Agencies must share resources, personnel, and programmatic functions in order to access the systems, technologies, tools, processes, and best practices required by the new architecture. Without accountability for sharing resources and implementing incremental changes on a universal timeframe, the future vision will not succeed. Successful adoption depends in large part on the active participation of all stakeholders.

3. Organize the national security declassification community into a federated National Declassification System (NDS), operating as a system-of-systems enterprise to streamline and modernize classification and declassification policies, processes, and technologies.

In the new paradigm, programmatic and technical requirements are necessary for the modernization of classification, declassification, and information management. The goal of these requirements will be to design a risk-based output-oriented architecture that supports timely public access to historically significant and permanently valuable information, and that implements modernized digital information management to aid end-users—especially Government policymakers and historians. The requirements will need to ensure that applicable information assurance and security are used to support both the appropriate protection of classified information, and to improve sharing throughout the records continuum model.[11]

4. Empower the NDC with the authorities and responsibilities to oversee the implementation of the NDS system-of-systems enterprise collective approach for managing classified information across the Executive branch and working with originating agencies.

   The NDC will require authorities to act, sanction, and fund the NDS. It must have oversight, tracking, and coordination responsibilities for the NDS. Leadership at the NDC should have sufficient inter-agency experience and qualifications, including the ability to perform Federal acquisition functions that support research, development and the deployment of new technologies necessary for realizing the long-term potential of the NDS.

Strategy to Achieve the Future Vision: Recommendations to Facilitate Strategic Technology Change

1. Transition to using technology, including tools and services for managing Big data, AI, Machine Learning, and Cloud storage and retrieval, to produce systems and services that support automated classification and declassification. This transition should institutionalize research and development activities across Government, incentivize private industry participation in these areas, and reform technology acquisition.

   Information Technology, and particularly tools and services that apply AI, Big Data, and Cloud solutions, among others are key to transitioning from the current analog model into a highly functioning digital paradigm. Agencies need to realign their IT resources appropriately using business-focused, data-driven analysis and technical evaluation. The Government-wide IT enterprise-level plan of action requires adjustable standardization that champions investment in research and development initiatives through partnerships. These partnerships should include advanced project agencies such as Intelligence Advanced Research Projects Activity (IARPA), Defense Advanced Research Projects Agency (DARPA) and Homeland Security Advanced Research Projects Agency (HSARPA) as well non-profit strategic ventures such as In-Q-Tel, the private sector and industry.

   For the IT cross-agency enterprise-level plan to advance, it is crucial to reform acquisition and contract management capabilities and practices. Incentivizing and rewarding public and private industry cross-agency priorities will drive efficient and agile business standards, coordinate acquisition requirements in business associate agreements (BAA), requests for information (RFI), and requests for proposals (RFP).

Immediate Impact: Recommendations for Near-Term Improvements to the Current System

The Government can take immediate action to improve the functioning of the current system while also preparing for the future of classification and declassification in a fully digital information environment. These high-impact recommendations support the goals of reducing over-classification and improving declassification in order to begin the transformation necessary for ensuring a credible and sustainable security classification system.

1. Direct the Secretary of Defense, the Director of National Intelligence, and the Secretary of Energy to assist the Archivist of the United States in modernizing the systems used across agencies for the management of classified records, including electronic records.

The Presidential Memorandum on Implementing Executive Order 13526 states that the President is "directing that the Secretary of Defense and the Director of National Intelligence each support research to assist the NDC in addressing the cross-agency challenges associated with declassification." Action on this tasking is long overdue. The NDC needs the assistance of the Secretary of Defense and the Director of National Intelligence in providing both resources and technical expertise to modernize the management of classified records.

2. Deploy technology to support classification and declassification automation.

When seeking new technologies, agencies must use a coordinated, Government-wide approach to better leverage resources and technical expertise. The use and sharing of technology to improve workflow should increase across the Government.[12] In addition to workflow tools, the Government remains in need of advanced technological tools to assist analysis and decision-making in support of declassification review. In our 2012 *Transforming Classification* Report to the President we underscored the importance of metadata standardization and data-tagging. It is essential to create a Government-wide metadata registry that remains critical in adopting and implementing technology solutions for classification and declassification. Lessons learned from the Intelligence Community's ongoing efforts focusing on the generation of classified data-tagging and classified metadata standards are critical for implementing AI technology solutions for classification (front-end) and declassification (back-end) of the classified information continuum. [13] Policy changes should support the adoption of these technologies, including advanced analytics and Machine Learning.

Revisions to Executive Order 13526 can provide the means to achieve these near-term goals and prepare the system for this future vision. The PIDB stands ready to assist the Records Access and Information Security Policy Coordination Committee at the National Security Council in its efforts to engage the interagency in revising the Order, and will continue to engage public interest groups, the "Sunshine in Government Community," and the public at large to advocate for transformation of the security classification system.

3. Implement secure information technology connectivity between and among all agencies managing classified information, specifically including NARA, which manages the NDC and classified records of the Presidential Libraries.

   Many agencies that hold classified information do not possess appropriate secure connectivity or networks to participate in a unified declassification program. This lack of connectivity and technology substantially impacts the equity recognition and referral process, with particularly negative consequences for the management of classified records at the NDC and the collections of the Presidential Libraries.

4. Direct the NDC to design and implement a process to solicit, evaluate, and prioritize topics for declassification across the Government, in dialog with Government agencies and the public.

   Establishing effective priorities that satisfy the widely varied needs and interests of researchers, the public, and Government agencies is not simple and will require senior-level decision-making. Public participation in this process will be critical to its success. Involving the public and stakeholders in determining priorities will be critical to the success of priority-based reviews that strengthen the credibility of a federated NDS.

5. Develop a new model for accurately measuring security classification activities across Government, including all costs associated with classification and declassification.

   The current methodology for measuring security classification activities remains woefully outdated and analog-based. At present, the data collected does not accurately portray the volume of information choking the security classification system, or account for the ways in which Government communicates using digital information. Without an accurate accounting of programmatic activities, determining appropriate resources for information management across Government will remain impossible.

An Executive Agency with the authority to develop a new methodological model would allow for accurate and consistent measurement of security classification activities, including declassification. Executive Order 13526 assigns the Information Security Oversight Office (ISOO) the responsibility for evaluating the effectiveness of the security classification programs of Executive branch agencies and industry, and reported in its Annual Report to the President. ISOO's 2017 Annual Report[14] recognized the shortcomings of current analog-based measurements. The Report noted the need to recalibrate and design more effective approaches to cost assessments and data collection that align with the digital transformation of Government and its corresponding new business practices.

The 2018 Annual Report noted that ISOO has started a process to reform and modernize its classification and declassification measurements.[15]

6. Simplify and streamline the classification system; decide how best to adopt a two-tiered classification system.

Led by the NSC, the RAIS PCC should conduct a study to decide how to adopt a simplified two-tier system. The study should require agencies to clearly identify and describe the harm anticipated in the event of an unauthorized disclosure. This will allow agencies to assess and categorize information by linking a clearly identifiable risk to an accurate harm assessment. Adopting a two-tiered model should not be difficult. In the digital environment today, classified information resides in either a SECRET system where information up to the SECRET level can be stored and disseminated, or a TOP SECRET system where information up to the TOP SECRET level can be stored and disseminated.". Agencies are beginning to rethink whether the use of CONFIDENTIAL is meaningful in the digital environment. A prime example of implementation has been the elimination of the CONFIDENTIAL level in NGA's security classification guide.[16]

The two classification levels would include access permission requirements to sensitive compartmented information (SCI) and special access program (SAP) information integrated into the system design, as is the current practice for SCI and SAP. TOP SECRET, the higher-level category, would afford a high level of protection and access permissions. All other classified information would be protected at the lower SECRET level using criteria for the lower level of access permissions. [17]

Additionally, the CUI program represents the President's order to standardize public access processes across the Executive branch so they correspond and are consistent with laws, regulations, and/or Government-wide policies. This instruction, once implemented in the next fiscal year, will enable timely and consistent information-sharing by properly protecting CUI from improper public release. Implementation plans include requirements for agencies to have appropriate access controls and handling caveats in their systems. In Fiscal Years 2019 and 2020, OMB required agencies to identify costs associated with implementation, and this requirement is included in the Fiscal Year 2021 budget process.

Endnotes

[1] *The President's Management Agenda*, 2018. https://www.whitehouse.gov/wp-content/uploads/2018/03/Presidents-Management-Agenda.pdf. Accessed July 17, 2018.

[2] Although the total costs of security classification activities is an unknowable figure, the cost estimates presented are those reported by agencies and departments to the Information Security Oversight Office (ISOO). ISOO Report to the President, 2017. https://www.archives.gov/files/isoo/reports/2017-annual-report.pdf. Accessed July 17, 2018.

[3] The precise measurement of digital information produced by the Government remains elusive. To garner perspective on the exponential rate of information creation across Government, the Barack Obama Presidential Library estimates that it holds 250 terabytes of digital information, a figure exponentially greater than the 80 terabytes held by the George W. Bush Presidential Library and Museum. The Clinton Presidential Library holds roughly 4 terabytes of digital information. See Figure 1.

[4] "System-of-systems" is the viewing of multiple, dispersed, independent systems in context as part of a larger, more complex system. A system is a group of interacting, interrelated and interdependent components that form a complex and unified whole. For a definition, see *TechTarget* at https://searchapparchitecture.techtarget.com/definition/system-of-systems-SoS. Accessed on January 2, 2018.

[5] "The Evolution of Systems Engineering," *Systems Engineering Guide*, The Mitre Corporation 1-11. http://www.mitre.org/sites/default/files/publications/se-guide-book-interactive.pdf. Accessed May 14, 2020. Accessed January 4, 2018.

[6] Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk GAO-17-63: Published: Dec 1, 2016. Publicly Released: Dec 1, 2016. https://www.gao.gov/products/GAO-17-63. Accessed May 14, 2020.

[7] For example, the National Geospatial-Intelligence Agency (NGA) recently completed a year-long project to consolidate all its security classification guides into a single guide, called the Consolidated National Geospatial-Intelligence Agency (CoNGA) Security Classification Guide (SCG) and then integrate its use into NGA systems. See an overview of the consolidation of security classification guides at https://www.archives.gov/files/isoo/fcgr/nga2017.pdf. Accessed July 17, 2018.

[8] "The Business of Artificial Intelligence," by Erik Brynjolfsson and Andrew McAfee, *Harvard Business Review,* August 7, 2017. https://hbr.org/cover-story/2017/07/the-business-of-artificial-intelligence. Accessed April 17, 2018.

[9] Techniques may include the use of Broad Agency Announcements (BAA), Other Transaction Authorities (OTA), Requests for Information (RFI), Requests for Quotations (RFQ), Requests for Proposals (RFP), and/or Indefinite Deliveries/Indefinite Quantities (IDIQ).

[10] The Office of Management and Budget (OMB) serves the President of the United States in overseeing the implementation of his vision across the Executive branch. Specifically, OMB's mission is to assist the President in meeting his policy, budget, management and regulatory objectives, and to fulfill the agency's statutory responsibilities. It carries out its mission through five critical processes that are essential to the President's ability to plan and implement his priorities across the Executive branch: 1. Budget development and execution. 2. Management, including oversight of agency performance, human capital, federal procurement, financial management, and information technology. 3. Regulatory policy, including coordination and review of all significant federal regulations by executive agencies. 4. Legislative clearance and coordination. 5. Executive Orders and Presidential Memoranda. https://www.whitehouse.gov/omb/. Accessed January 20, 2018.

[11] The records continuum model is a model of archival science that emphasizes overlapping characteristics of recordkeeping, evidence, transaction, and the identity of the creator. It deemphasizes the time-bound stages of the life cycle model. A continuum-based approach suggests integrated time-space dimensions. Records are 'fixed' in time and space from the moment of their creation, but record-keeping regimes carry them forward and enable their use for multiple purposes by delivering them to people living in different times and spaces. *A Glossary of Archival and Records Terminology,* Society of American Archivists. https://www2.archivists.org/glossary. Accessed January 2, 2018.

[12] A benefit to investing and adopting advanced technologies as part of a robust information management system would incorporate solutions to modernize and improve Freedom of Information Act (FOIA) processes. "The Intelligence Community Office of Inspector General (IC OIG) issued a report titled, Assessment of IC Freedom of Information Act (FOIA) Programs, in September 2018 and publicly released in November, 2018. https://www.dni.gov/files/ICIG/Documents/Publications/Reports/2018/IC%20FOIA%20Programs/ICIG_Assess_IC_FOIA_Programs_INS-2018-01-U.pdf. Several of the IC OIG's Findings and recommendations for FOIA improvements echo recommendations in this report. They include the need for: 1) DNI leadership to better support interagency integration and collaboration; 2) the use of information technologies to facilitate the interagency referral and consultation process; and 3) DNI support to lead development of a secure virtual collaboration space. The IC OIG report highlighted the fact that not all IC agency FOIA offices have the ability to electronically transmit records under review to other agencies. Like the NDC and many other agency declassification offices, these IC FOIA offices lack access to the Joint Worldwide Intelligence Communications System (JWICS). Access to JWICS would enable significantly more efficient declassification and FOIA review of Top Secret information that otherwise must be hand-carried between agencies.

[13] See Recommendation 13 in Transforming the Security Classification System: Report to the President from the Public Interest Declassification Board, November 2012. https://www.archives.gov/files/declassification/pidb/recommendations/transforming-classification.pdf. Accessed July 17, 2018.

[14] https://www.archives.gov/files/isoo/reports/2017-annual-report.pdf. February 25, 2020.

[15] https://www.archives.gov/files/isoo/images/2018-isoo-annual-report.pdf. Accessed February 25, 2020.

[16] See Endnote 7. For a discussion of a two-tiered model, see Recommendation 3 of Transforming the Security Classification System: Report to the President from the Public Interest Declassification Board, November 2012. https://www.archives.gov/declassification/pidb/recommendations/transforming-classification.html. Accessed July 17, 2018.

[17] For additional information on this recommendation, see: Transforming the Security Classification System: Report to the President from the Public Interest Declassification Board, November 2012. https://www.archives.gov/files/declassification/pidb/recommendations/transforming-classification.pdf. Accessed July 17, 2018. The PIDB's second and third recommendations in this earlier report advocate for simplification of the classification system.

Appendix A

Biographies

Contributing Current Members

Presidential Appointees

James E. Baker was appointed by President Barack Obama on June 22, 2016, and served as Acting Chairman in 2018 and 2020. Judge Baker retired from the United States Court of Appeals for the Armed Forces in July 2015 after fifteen years of service, the last four as Chief Judge. Judge Baker is currently a Professor at the Syracuse University College of Law and the Maxwell School of Citizenship and Public Affairs where he also serves as Director of the Syracuse University Institute for Security Policy and Law.. He previously served as the Robert J. Wilhelm Fellow at the Massachusetts Institute of Technology (2017–2018) and Chair of the ABA Standing Committee on Law and National Security (2015–2018). He previously served as Special Assistant to the President and Legal Adviser to the National Security Council (NSC) (1997–2000), Deputy Legal Adviser to the National Security Council (1994–1997) and as Counsel to the President's Foreign Intelligence Advisory Board and Intelligence Oversight Board. Judge Baker has also served as an attorney adviser in the Office of the Legal Advisor, Department of State, a legislative aide and acting Chief of Staff to Senator Daniel Patrick Moynihan (1985–1987), and as a Marine Corps infantry officer, resigning his Reserve commission upon joining the United States Court of Appeals for the Armed Forces. He is the author of *In the Common Defense: National Security Law for Perilous Times* (Cambridge: 2007) and, with Michael Riesman, *Regulating Covert Action* (Yale University Press: 1992). He received a B.A from Yale University and a J.D. from Yale Law School. He is serving his first term on the PIDB.

Trevor W. Morrison was appointed by President Barack Obama on June 22, 2016, serving as Chairman from his appointment date until June 21, 2018. Mr. Morrison is currently the Dean and Eric M. and Laurie B. Roth Professor of Law at New York University School of Law, where he is also faculty co-director of the Reiss Center on Law and Security. He was previously the Liviu Librescu Professor of Law at Columbia Law School. Mr. Morrison spent 2009 in the White House, where he served as associate counsel to President Barack Obama. Before entering academia, he was a law clerk to Judge Betty B. Fletcher of the U.S. Court of Appeals for the Ninth Circuit (1998-99) and to Justice Ruth Bader Ginsburg of the U.S. Supreme Court (2002-03). Between those clerkships, he was a Bristow Fellow in the U.S. Justice Department's Office of the Solicitor General (1999–2000), an attorney-advisor in the Justice Department's Office of Legal Counsel (2000-01), and an associate at Wilmer, Cutler & Pickering (now WilmerHale) (2001-02). Mr. Morrison is a Fellow of the American Academy of Arts and Sciences and a member of the American Law

Institute and the Council on Foreign Relations. He received a B.A. (hons.) in history from the University of British Columbia in 1994, and a J.D. from Columbia Law School in 1998. Mr. Morrison is serving his first term on the PIDB.

Congressional Appointees

Alissa M. Starzak was appointed by Charles E. Schumer, Minority Leader of the Senate on February 27, 2018. Presently, Ms. Starzak is Head of Public Policy at Cloudflare, a web security and optimization company. Prior to joining Cloudflare, she worked for the U.S government in a variety of national security positions. Most recently, she served as the 21st General Counsel of the Department of the Army, after confirmation by the Senate. As General Counsel of the Army, she was the primary legal counsel to the Secretary of the Army and the Army's chief legal officer. Before her appointment as Army General Counsel, Ms. Starzak served as the Deputy General Counsel (Legislation) of the U.S. Department of Defense, advising on legal issues with a legislative or congressional component and managing an office of attorneys responsible for developing the Department of Defense legislative program. Prior to moving to the Department of Defense, she served as Counsel to the Senate Select Committee on Intelligence, focusing on legal issues relating to intelligence collection and covert action, and as an Assistant General Counsel at the Central Intelligence Agency's Office of General Counsel. She also worked in private practice in Washington, D.C., and clerked for The Honorable E. Grady Jolly, U.S. Court of Appeals for the Fifth Circuit. She graduated from Amherst College and the University of Chicago Law School, where she served as an editor of the University of Chicago Law Review. Ms. Starzak is serving her first term on the PIDB.

John F. Tierney was appointed by Nancy Pelosi as Minority Leader of the House of Representatives on July 20, 2017. He is presently Executive Director at the Center for Arms Control & Non-Proliferation and its sister organization, The Council for a Livable World. His work focuses on national security issues, nuclear non-proliferation, missile defense and areas concerning peace and security. Mr. Tierney is a former nine-term Massachusetts Congressman who served on the House Permanent Select Commitee on Intelligence and chaired the National Security and Foreign Affairs Subcommittee of the Government Oversight and Reform Committee. His 18-year career included oversight of the Government Accountability Office's annual assessment of the Pentagon's Weapons Selection Programs and reform of overall Pentagon spending. Additionally, Mr. Tierney was a senior member of the Education and Workforce Committee of the House, where he served as Ranking Member on the Health,

Employment, Labor and Pension Subcommittee, and served on the Higher Education and Workforce Development Committee where he had a prominent role in several Higher Education Reauthorization and Workforce Opportunity Reauthorization Acts and related legislation. Prior to being elected to Congress, Mr. Tierney was a Partner in the law firm Tierney, Kalis and Lucas, counsel for several community governments, a Trustee of Salem State College (now University) and member and President of the local Chamber of Commerce. He holds a B.A. from Salem State College and J.D. from Suffolk University Law School. Mr. Tierney is serving his first term on the PIDB.

Kenneth L. Wainstein was appointed by Mitch McConnell as Minority Leader of the Senate on September 20, 2016. He currently is a partner at Davis Polk & Wardwell LLP. He is an adjunct professor of law at the Georgetown University Center of Law. Mr. Wainstein previously was a partner at Cadwalader, Wickersham & Taft LLP. Mr. Wainstein served as an Assistant U.S. Attorney, first in the Southern District of New York and then in the District of Columbia. In 2001, he served as the Director of the Executive office for U.S. Attorneys. In 2002, Mr. Wainstein joined the Federal Bureau of Investigation as General Counsel. FBI Director Robert S. Mueller appointed him Chief of Staff in 2003. Mr. Wainstein was appointed by President George W. Bush to serve as the United States Attorney for the District of Columbia in 2004, a position he held until his appointment as Assistant Attorney General for National Security at the Justice Department in 2006. As the first Assistant Attorney General for National Security, he established and led the new National Security Division, which consolidated the Justice Department's law enforcement and intelligence activities on counter-terrorism and counterintelligence matters. In 2008, after 19 years at the Justice Department, Mr. Wainstein was named Homeland Security Advisor by President George W. Bush. As the Assistant to the President for Homeland Security and Counter-Terrorism, he advised the President on all homeland security matters, chaired the Homeland Security Council, and oversaw the inter-agency coordination process for homeland security and counter-terrorism programs. Mr. Wainstein holds a B.A. from the University of Virginia and a J.D. from the University of California, Berkeley. Mr. Wainstein is serving his second term on the PIDB.

Contributing Former Members

Laura A. DeBonis was appointed by President Barack Obama in March 2015 and served one term until March 2018. Ms. DeBonis has over 20 years' experience in the information technology and media fields. She currently serves as a founding Board Member for the Digital Public Library of America, an organization dedicated to creating an open network of online resources from libraries, archives and museums and making them freely available to all. Her professional experience includes a variety of leadership roles at Google, including her last position there as the Director of Library Partnerships for Book Search. Since Google,

Ms. DeBonis has been a consultant to a number of organizations, including serving as chair of the technology review team for the Internet Safety Technical Task Force at the Berkman Center at Harvard University. DeBonis is an emeritus trustee for WGHB Boston and previously served on the board of the Boston Public Library. She received a B.A. from Harvard College and an M.B.A. from Harvard Business School.

Martin C. Faga was appointed by President George W. Bush in October 2004 and served three terms until October 2014. He was the President and Chief Executive Officer of The MITRE Corporation for six years, retiring in 2006. Before joining MITRE, Mr. Faga served as Assistant Secretary of the Air Force for Space from 1989 until 1993. At the same time, he served as Director of the National Reconnaissance Office, responsible to the Secretary of Defense and the Director of Central Intelligence for the development, acquisition, and operation of all U.S. satellite reconnaissance programs. Mr. Faga has been awarded the National Intelligence Distinguished Service Medal, the Department of Defense Distinguished Public Service Medal, the Air Force Exceptional Civilian Service Medal, and the NASA Distinguished Service Medal. In 2004, he was awarded the Intelligence Community Seal Medallion. He was first appointed to the Board in October 2004, and again in January 2009. He has also served on the President's Intelligence Advisory Board. Mr. Faga graduated from Lehigh University with a B.S. and an M.S. in electrical engineering.

William H. Leary was appointed by President Barack Obama in February 2012 and served two terms until January 2018. He was the Special Adviser to the National Security Advisor and Senior Director for Records and Access Management on the National Security Staff until his retirement in 2011. In that capacity, he had served as Chair of the Interagency Security Classification Appeals Panel and Chair of the Records Access and Information Security Interagency Policy Committee. A strong proponent of governmental transparency, Mr. Leary was one of the primary Executive branch officials behind the creation of the PIDB in 2000 and the development of President Obama's Executive Order 13526 on Classified National Security Information. Prior to joining the National Security Council staff, he served as the Deputy Director of the Agency Services Division at the National Archives and Records Administration for five years. From 1968 until 1973, Mr. Leary taught American history at the University of Virginia, the College of William and Mary, and the University of South Alabama. He received his B.A. in foreign affairs and M.A. and A.B.D. in history, all from the University of Virginia.

David E. Skaggs was appointed by Nancy Pelosi as Minority Leader House of Representatives in January 2005 and served three terms until March 2015. He is the Chairman of the board of the Office of Congressional Ethics and former (2007–2009) Executive Director of the Colorado Department of Higher Education. He served 12 years in Congress (1987–1999) as the Representative from the 2nd Congressional District in Colorado, including 8 years on the House Appropriations Committee and 6 years on the House Permanent Select Committee on Intelligence. After leaving Congress, he served as Executive Director of the Center for Democracy and Citizenship at the Council for Excellence in Government (1999–2006), counsel to a

Washington, DC-based law firm, and 3 years as an adjunct professor at the University of Colorado. He has a B.A. in philosophy from Wesleyan University and an LL.B from Yale Law School.

Admiral William O. Studeman, USN (Ret.) was appointed by John Boehner as the Speaker of the House in June 2006 and served three terms until May of 2015. He retired from Northrop Grumman Corporation as Vice President and Deputy General Manager of Mission Systems. Admiral Studeman's flag tours included OPNAV Director of Long Range Navy Planning; Director of Naval Intelligence; Director of the National Security Agency; and Deputy Director of the Central Intelligence Agency, with two extended periods as Acting Director. He served as a member of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction and is currently serving on the National Advisory Board on Bio-Security and the Defense Science Board. He holds a B.A. in history from the University of the South in Sewanee, TN, and an M.A. in public and international affairs from George Washington University.

Solomon B. Watson IV was appointed by President Barack Obama in March 2015 and served one term until March 2018. He was Senior Vice President and Chief Legal Officer of The New York Times Company, positions he held from 2005 to 2006. He began his career at The New York Times Company in 1974 and held various positions including Senior Vice President and General Counsel from 1996 to 2005, Vice President and General Counsel from 1990 to 1996, General Counsel from 1989 to 1990, Corporate Secretary from 1979 to 1989 and 2000 to 2002, and Corporate Counsel from 1974 to 1979. Mr. Watson has been a Special Master in the Appellate Division of the New York State Supreme Court and a member of the American Bar Association, the National Bar Association, and the Association of the Bar of the City of New York. From 1966 to 1968 he served in the U.S. Army as a lieutenant in the Military Police Corps and was awarded the Bronze Star and Army Commendation Medals for his service while in Vietnam. Mr. Watson received a B.A. from Howard University and a J.D. from Harvard Law School.

Appendix B

Public Interest Declassification Act of 2000, as amended

See: Public Law 106-567 (December 27, 2000)

SEC. 701. SHORT TITLE.

This title may be cited as the "Public Interest Declassification Act of 2000".

SEC. 702. FINDINGS.

Congress makes the following findings:

(1) It is in the national interest to establish an effective, coordinated, and cost-effective means by which records on specific subjects of extraordinary public interest that do not undermine the national security interests of the United States may be collected, retained, reviewed, and disseminated to Congress, policymakers in the executive branch, and the public.

(2) Ensuring, through such measures, public access to information that does not require continued protection to maintain the national security interests of the United States is a key to striking the balance between secrecy essential to national security and the openness that is central to the proper functioning of the political institutions of the United States.

SEC. 703. PUBLIC INTEREST DECLASSIFICATION BOARD.

(a) ESTABLISHMENT. —

(1) There is established within the executive branch of the United States a board to be known as the "Public Interest Declassification Board" (in this title referred to as the"Board").

(2) The Board shall report directly to the President or, upon designation by the President, the Vice President, the Attorney General, or other designee of the President. The other designee of the President under this paragraph may not be an agency head or official authorized to classify information under Executive Order 12958, or any successor order.

(b) PURPOSES. — The purposes of the Board are as follows:

(1) To advise the President, the Assistant to the President for National Security Affairs, the Director of the Office of Management and Budget, and such other executive branch officials as the Board consid-

ers appropriate on the systematic, thorough, coordinated, and comprehensive identification, collection, review for declassification, and release to Congress, interested agencies, and the public of declassified records and materials (including donated historical materials) that are of archival value, including records and materials of extraordinary public interest.

(2) To promote the fullest possible public access to a thorough, accurate, and reliable documentary record of significant United States national security decisions and significant United States national security activities in order to—

(A) support the oversight and legislative functions of Congress;

(B) support the policymaking role of the executive branch;

(C) respond to the interest of the public in national security matters; and

(D) promote reliable historical analysis and new avenues of historical study in national security matters.

(3) To provide recommendations to the President for the identification, collection, and review for declassification of information of extraordinary public interest that does not undermine the national security of the United States, to be undertaken in accordance with a declassification program that has been established or may be established by the President by Executive order.

(4) To advise the President, the Assistant to the President for National Security Affairs, the Director of the Office of Management and Budget, and such other executive branch officials as the Board considers appropriate on policies deriving from the issuance by the President of Executive orders regarding the classification and declassification of national security information.

(5) To review and make recommendations to the President in a timely manner with respect to any congressional request, made by the committee of jurisdiction or by a member of the committee of jurisdiction, to declassify certain records, to evaluate the proper classification of certain records, or to reconsider a declination to declassify specific records.

(c) MEMBERSHIP. —

(1) The Board shall be composed of nine individuals appointed from among citizens of the United States who are preeminent in the fields of history, national security, foreign policy, intelligence policy, social science, law, or archives, including individuals who have served in Congress or otherwise in the Federal Government or have otherwise engaged in research, scholarship, or publication in such fields on matters relating to the national security of the United States, of whom—

(A) five shall be appointed by the President;

(B) one shall be appointed by the Speaker of the House of Representatives;

(C) one shall be appointed by the majority leader of the Senate;

(D) one shall be appointed by the minority leader of the Senate; and

(E) one shall be appointed by the minority leader of the House of Representatives.

(2) (A) Of the members initially appointed to the Board by the President—

(i) three shall be appointed for a term of 4 years;

(ii) one shall be appointed for a term of 3 years; and

(iii) one shall be appointed for a term of 2 years.

(B) The members initially appointed to the Board by the Speaker of the House of Representatives or by the majority leader of the Senate shall be appointed for a term of 3 years.

(C) The members initially appointed to the Board by the minority leader of the House of Representatives or the Senate shall be appointed for a term of 2 years.

(D) Any subsequent appointment to the Board shall be for a term of 3 years from the date of the appointment.

(3) A vacancy in the Board shall be filled in the same manner as the original appointment.

(4) A member of the Board may be appointed to a new term on the Board upon the expiration of the member's term on the Board, except that no member may serve more than three full terms on the Board.

(d) CHAIRPERSON; EXECUTIVE SECRETARY. —

(1) (A) The President shall designate one of the members of the Board as the chairperson of the Board.

(B) The term of service as Chairperson of the Board shall be 2 years.

(C) A member serving as Chairperson of the Board may be redesignated as Chairperson of the Board upon the expiration of the member's term as Chairperson of the Board, except that no member shall serve as Chairperson of the Board for more than 6 years.

(2) The Director of the Information Security Oversight Office shall serve as the Executive Secretary of the Board.

(e) MEETINGS. — The Board shall meet as needed to accomplish its mission, consistent with the availability of funds, but shall meet in person not less frequently than on a quarterly basis.. A majority of the members of the Board shall constitute a quorum.

(f) STAFF. — Any employee of the Federal Government may be detailed to the Board, with the agreement of and without reimbursement to the detailing agency, and such detail shall be without interruption or loss of civil, military, or foreign service status or privilege.

(g) SECURITY. —

(1) The members and staff of the Board shall, as a condition of appointment to or employment with the Board, hold appropriate security clearances for access to the classified records and materials to be reviewed by the Board or its staff, and shall follow the guidance and practices on security under applicable Executive orders and Presidential or agency directives.

(2) The head of an agency shall, as a condition of granting access to a member of the Board, the Executive Secretary of the Board, or a member of the staff of the Board to classified records or materials of the agency under this title, require the member, the Executive Secretary, or the member of the staff, as the case may be, to—

(A) execute an agreement regarding the security of such records or materials that is approved by the head of the agency; and

(B) hold an appropriate security clearance granted or recognized under the standard procedures and eligibility criteria of the agency, including any special access approval required for access to such records or materials.

(3) The members of the Board, the Executive Secretary of the Board, and the members of the staff of the Board may not use any information acquired in the course of their official activities on the Board for nonofficial purposes.

(4) For purposes of any law or regulation governing access to classified information that pertains to the national security of the United States, and subject to any limitations on access arising under section 706(b), and to facilitate the advisory functions of the Board under this title, a member of the Board seeking access to a record or material under this title shall be deemed for purposes of this subsection to have a need to know the contents of the record or material.

(h) COMPENSATION. —

(1) Each member of the Board shall receive compensation at a rate not to exceed the daily equivalent of the annual rate of basic pay payable for positions at ES–1 of the Senior Executive Service under section 5382 of title 5, United States Code, for each day such member is engaged in the actual performance of duties of the Board.

(2) Members of the Board shall be allowed travel expenses, including per diem in lieu of subsistence at rates authorized for employees of agencies under subchapter I of chapter 57 of title 5, United States Code, while away from their homes or regular places of business in the performance of the duties of the Board.

(i) GUIDANCE; ANNUAL BUDGET. —

(1) On behalf of the President, the Assistant to the President for National Security Affairs shall provide guidance on policy to the Board.

(2) The Executive Secretary of the Board, under the direction of the Chairperson of the Board and the Board, and acting in consultation with the Archivist of the United States, the Assistant to the President for National Security Affairs, and the Director of the Office of Management and Budget, shall prepare the annual budget of the Board.

(j) SUPPORT. — The Information Security Oversight Office may support the activities of the Board under this title. Such support shall be provided on a reimbursable basis.

(k) PUBLIC AVAILABILITY OF RECORDS AND REPORTS. —

(1) The Board shall make available for public inspection records of its proceedings and reports prepared in the course of its activities under this title to the extent such records and reports are not classified and would not be exempt from release under the provisions of section 552 of title 5, United States Code.

(2) In making records and reports available under paragraph (1), the Board shall coordinate the release of such records and reports with appropriate officials from agencies with expertise in classified information in order to ensure that such records and reports do not inadvertently contain classified information.

(l) APPLICABILITY OF CERTAIN ADMINISTRATIVE LAWS. — The provisions of the Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the activities of the Board under this title. However, the records of the Board shall be governed by the provisions of the Federal Records Act of 1950.

SEC. 704. IDENTIFICATION, COLLECTION, AND REVIEW FOR DECLASSIFICATION OF INFORMATION OF ARCHIVAL VALUE OR EXTRAORDINARY PUBLIC INTEREST.

(a) BRIEFINGS ON AGENCY DECLASSIFICATION PROGRAMS. —

(1) As requested by the Board, or by the Select Committee on Intelligence of the Senate or the Permanent Select Committee on Intelligence of the House of Representatives, the head of any agency with the authority under an Executive order to classify information shall provide to the Board, the Select Committee on Intelligence of the Senate, or the Permanent Select Committee on Intelligence of the House of Representatives, on an annual basis, a summary briefing and report on such agency's progress and plans in the declassification of national security information. Such briefing shall cover the declassification goals set by statute, regulation, or policy, the agency's progress with respect to such goals, and the agency's planned goals and priorities for its declassification activities over the next 2 fiscal years. Agency briefings and reports shall give particular attention to progress on the declassification of records and materials that are of archival value or extraordinary public interest to the people of the United States.

(2)(A) The annual briefing and report under paragraph (1) for agencies within the Department of Defense, including the military departments and the elements of the intelligence community, shall be provided on a consolidated basis.

(B) In this paragraph, the term "elements of the intelligence community" means the elements of the intelligence community specified or designated under section 3(4) of the National Security Act of 1947 (50 U.S.C. 401a(4)).

(b) RECOMMENDATIONS ON AGENCY DECLASSIFICATION PROGRAMS. —

(1) Upon reviewing and discussing declassification plans and progress with an agency, the Board shall provide to the head of the agency the written recommendations of the Board as to how the agency's declassification program could be improved. A copy of each recommendation shall also be submitted to the Assistant to the President for National Security Affairs and the Director of the Office of Management and Budget.

(2) Consistent with the provisions of section 703(k), the Board's recommendations to the head of an agency under paragraph (1) shall become public 60 days after such recommendations are sent to the head of the agency under that paragraph.

(c) RECOMMENDATIONS ON SPECIAL SEARCHES FOR RECORDS OF EXTRAORDINARY PUBLIC INTEREST. —

(1) The Board shall also make recommendations to the President regarding proposed initiatives to identify, collect, and review for declassification classified records and materials of extraordinary public interest.

(2) In making recommendations under paragraph (1), the Board shall consider the following:

(A) The opinions and requests of Members of Congress, including opinions and requests expressed or embodied in letters or legislative proposals, and also including specific requests for the declassification of certain records or for the reconsideration of declinations to declassify specific records.

(B) The opinions and requests of the National Security Council, the Director of National Intelligence, and the heads of other agencies.

(C) The opinions of United States citizens.

(D) The opinions of members of the Board.

(E) The impact of special searches on systematic and all other on-going declassification programs.

(F) The costs (including budgetary costs) and the impact that complying with the recommendations would have on agency budgets, programs, and operations.

(G) The benefits of the recommendations.

(H) The impact of compliance with the recommendations on the national security of the United States.

(d) PRESIDENT'S DECLASSIFICATION PRIORITIES. —

(1) Concurrent with the submission to Congress of the budget of the President each fiscal year under section 1105 of title 31, United States Code, the Director of the Office of Management and Budget shall publish a description of the President's declassification program and priorities, together with a listing of the funds requested to implement that program.

(2) Nothing in this title shall be construed to substitute or supersede, or establish a funding process for, any declassification program that has been established or may be established by the President by Executive order.

(e) DECLASSIFICATION REVIEWS. —

(1) IN GENERAL – If requested by the President, the Board shall review in a timely manner certain records or declinations to declassify specific records, the declassification
of which has been the subject of specific congressional request described in section 703(b)(5).

(2) AUTHORITY OF THE BOARD – Upon receiving a congressional request described in section 703(b)(5), the Board may conduct the review and make the recommendations described in that section, regardless of whether such a review is requested by the President.

(3) REPORTING – Any recommendations submitted to the President by the Board under section 703(b)(5), shall be submitted to the chairman and ranking minority member of the committee of Congress that made the request relating to such recommendations.

SEC. 705. PROTECTION OF NATIONAL SECURITY INFORMATION AND OTHER INFORMATION.

(a) IN GENERAL. — Nothing in this title shall be construed to limit the authority of the head of an agency to classify information or to continue the classification of information previously classified by that agency.

(b) SPECIAL ACCESS PROGRAMS. — Nothing in this title shall be construed to limit the authority of the head of an agency to grant or deny access to a special access program.

(c) AUTHORITIES OF DIRECTOR OF NATIONAL INTELLIGENCE. — Nothing in this title shall be construed to limit the authorities of the Director of National Intelligence as the head of the intelligence community,

including the Director's responsibility to protect intelligence sources and methods from unauthorized disclosure as required by section 103(c)(6) of the National Security Act of 1947 (50 U.S.C. 403–3(c)(6)).

(d) EXEMPTIONS TO RELEASE OF INFORMATION. — Nothing in this title shall be construed to limit any exemption or exception to the release to the public under this title of information that is protected under subsection (b) of section 552 of title 5, United States Code (commonly referred to as the "Freedom of Information Act"), or section 552a of title 5, United States Code (commonly referred to as the "Privacy Act").

(e) WITHHOLDING INFORMATION FROM CONGRESS. — Nothing in this title shall be construed to authorize the withholding of information from Congress.

SEC. 706. STANDARDS AND PROCEDURES.

(a) LIAISON. —

(1) The head of each agency with the authority under an Executive order to classify information and the head of each Federal Presidential library shall designate an employee of such agency or library to act as liaison to the Board for purposes of this title.

(2) The Board may establish liaison and otherwise consult with such other historical and advisory committees as the Board considers appropriate for purposes of this title.

(b) LIMITATIONS ON ACCESS. —

(1) (A) Except as provided in paragraph (2), if the head of an agency or the head of a Federal Presidential library determines it necessary to deny or restrict access of the Board, or of the agency or library liaison to the Board, to information contained in a record or material, in whole or in part, the head of the agency or the head of the library shall promptly notify the Board in writing of such determination.

(B) Each notice to the Board under subparagraph (A) shall include a description of the nature of the records or materials, and a justification for the determination, covered by such notice.

(2) In the case of a determination referred to in paragraph (1) with respect to a special access program created by the Secretary of Defense, the Director of National Intelligence, or the head of any other agency, the notification of denial of access under paragraph (1), including a description of the nature of the Board's request for access, shall be submitted to the Assistant to the President for National Security Affairs rather than to the Board.

(c) DISCRETION TO DISCLOSE. — At the conclusion of a declassification review, the head of an agency may, in the discretion of the head of the agency, determine that the public's interest in the disclosure of records or materials of the agency covered by such review, and still properly classified, outweighs the Government's need to protect such records or materials, and may release such records or materials in accordance with the provisions of Executive Order No. 12958 or any successor order to such Executive order.

(d) DISCRETION TO PROTECT. — At the conclusion of a declassification review, the head of an agency may, in the discretion of the head of the agency, determine that the interest of the agency in

the protection of records or materials of the agency covered by such review, and still properly classified, outweighs the public's need for access to such records or materials, and may deny release of such records or materials in accordance with the provisions of Executive Order No. 12958 or any successor order to such Executive order.

(e) REPORTS. —

(1) (A) Except as provided in paragraph (2), the Board shall annually submit to the appropriate congressional committees a report on the activities of the Board under this title, including summary information regarding any denials to the Board by the head of an agency or the head of a Federal Presidential library of access to records or materials under this title.

(B) In this paragraph, the term "appropriate congressional committees" means the Select Committee on Intelligence and the Committee on Governmental Affairs of the Senate and the Permanent Select Committee on Intelligence and the Committee on Government Reform of the House of Representatives.

(2) Notwithstanding paragraph (1), notice that the Board has been denied access to records and materials, and a justification for the determination in support of the denial, shall be submitted by the agency denying the access as follows:

(A) In the case of the denial of access to a special access program created by the Secretary of Defense, to the Committees on Armed Services and Appropriations of the Senate and to the Committees on Armed Services and Appropriations of the House of Representatives.

(B) In the case of the denial of access to a special access program created by the Director of National Intelligence, or by the head of any other agency (including the Department of Defense) if the special access program pertains to intelligence activities, or of access to any information and materials relating to intelligence sources and methods, to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives.

(C) In the case of the denial of access to a special access program created by the Secretary of Energy or the Administrator for Nuclear Security, to the Committees on Armed Services and Appropriations and the Select Committee on Intelligence of the Senate and to the Committees on Armed Services and Appropriations and the Permanent Select Committee on Intelligence of the House of Representatives.

(f) NOTIFICATION OF REVIEW. — In response to a specific congressional request for declassification review described in section 703(b)(5), the Board shall advise the originators of the request in a timely manner whether the Board intends to conduct such review.

SEC. 707. JUDICIAL REVIEW.

Nothing in this title limits the protection afforded to any information under any other provision of law. This title is not intended and may not be construed to create any right or benefit, substantive or procedural,

enforceable against the United States, its agencies, its officers, or its employees. This title does not modify in any way the substantive criteria or procedures for the classification of information, nor does this title create any right or benefit subject to judicial review.

SEC. 708. FUNDING.

(a) AUTHORIZATION OF APPROPRIATIONS. — There is hereby authorized to be appropriated to carry out the provisions of this title amounts as follows:

(1) For fiscal year 2001, $650,000.

(2) For each fiscal year after fiscal year 2001, such sums as may be necessary for such fiscal year.

(b) FUNDING REQUESTS. — The President shall include in the budget submitted to Congress for each fiscal year under section 1105 of title 31, United States Code, a request for amounts for the activities of the Board under this title during such fiscal year.

SEC. 709. DEFINITIONS.

In this title:

(1) AGENCY.—

(A) Except as provided in subparagraph (B), the term "agency" means the following:

(i) An Executive agency, as that term is defined in section 105 of title 5, United States Code.

(ii) A military department, as that term is defined in section 102 of such title.

(iii) Any other entity in the executive branch that comes into the possession of classified information.

(B) The term does not include the Board.

(2) CLASSIFIED MATERIAL OR RECORD.— The terms "classified material" and "classified record" include any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microfilm, sound recording, videotape, machine readable records, and other documentary material, regardless of physical form or characteristics, that has been determined pursuant to Executive order to require protection against unauthorized disclosure in the interests of the national security of the United States.

(3) DECLASSIFICATION.—The term "declassification" means the process by which records or materials that have been classified are determined no longer to require protection from unauthorized disclosure to protect the national security of the United States.

(4) DONATED HISTORICAL MATERIAL.—The term "donated historical material" means collections of personal papers donated or given to a Federal Presidential library or other archival repository under a deed of gift or otherwise.

(5) FEDERAL PRESIDENTIAL LIBRARY.—The term "Federal Presidential library" means a library operated and maintained by the United States Government through the National Archives and Records Administration under the applicable provisions of the Federal Records Act of 1950.

(6) NATIONAL SECURITY.—The term "national security" means the national defense or foreign relations of the United States.

(7) RECORDS OR MATERIALS OF EXTRAORDINARY PUBLIC INTEREST.—The term "records or materials of extraordinary public interest" means records or materials that—

(A) demonstrate and record the national security policies, actions, and decisions of the United States, including—

(i) policies, events, actions, and decisions which led to significant national security outcomes; and

(ii) the development and evolution of significant United States national security policies, actions, and decisions;

(B) will provide a significantly different perspective in general from records and materials publicly available in other historical sources; and

(C) would need to be addressed through ad hoc record searches outside any systematic declassification program established under Executive order.

(8) RECORDS OF ARCHIVAL VALUE.—The term "records of archival value" means records that have been determined by the Archivist of the United States to have sufficient historical or other value to warrant their continued preservation by the Federal Government.

SEC. 710. EFFECTIVE DATE.

This title shall take effect on the date that is 120 days after the date of the enactment of this Act.

Appendix C

The Importance of Technology in Classification and Declassification
A White Paper of the Public Interest Declassification Board
June 2016

Introduction to the PIDB Declassification Technology Working Group

At the direction of the President, the Public Interest Declassification Board (PIDB) continues to investigate technologies and related policy solutions to transform the security classification system to one capable of functioning more effectively in an increasingly complex information age.[1] Core to our democratic ideals is the ability for the public to access its government's records. The responsibility lies with senior government leaders to develop sound policies and implement technological capabilities that will ensure long-term preservation and accessibility to the nation's historical records. Nearly all users of the security classification system agree that it is no longer able to handle the current volume and forms of information, especially given the exponential growth of digital information that is only exacerbating the many challenges facing the system. **As the PIDB has previously noted in all of our reports, we reaffirm that our most important recommendation for developing and ensuring such a system is the adoption of a government-wide technology investment strategy for the management of classified information.**

In support of this recommendation and those commitments found in the President's *Open Government National Action Plans*, the PIDB began an in-depth study of agency declassification technology initiatives last year. In May 2015, we established an informal Declassification Technology Working Group (Working Group) at the National Archives and asked for agency participation in a high-level questionnaire concerning agency preparedness for declassification in the digital age. We sought support from agency Chief Information Officers (CIOs) when setting up the Working Group in order to highlight declassification technology development as a need for agencies. We believe the support of agency CIOs is critical to modernizing declassification and making the management of classified information at agencies a priority in planning their information technology programs now and in the years ahead.

The Working Group has representation from technologists at 14 agencies and departments in the Executive Branch. The PIDB hosted four Working Group meetings in the past year. These meetings are an opportunity for agencies to share their successes, challenges, best practices, requirements and declassification program needs. Agenda items covered at these meetings included agencies briefings on their efforts at declassification technology planning, discussions of best practices concerning the management of classified records

(including email), the sharing of metadata standards and transfer guidance, and more. We have received positive feedback from agencies about the usefulness of meeting in this informal Working Group environment; agency technologists are able to work collaboratively, share best practices and discuss new ideas with their inter-agency counterparts on these often overlooked technology challenges.

Now, at the one-year anniversary of the beginning of our Working Group exercise, we have collected some observations and lessons-learned to share from these meetings with the public. Our goal is to reflect on the progress of the Working Group and plan next steps and potential areas in need of further study.

Finding the Baseline: Where Agencies Stand

Overall, agencies lack appropriate technological investment to support the activities of their declassification and related records management programs. Most agencies do not possess basic workflow applications to assist human review of records, applications that are readily available in the commercial world. While one or two agencies are exploring advanced content understanding and analytics as technical capabilities to assist review, the vast majority of agencies lack the most basic technological infrastructure to support simple automation or search technologies to assist in the management of records through the review process.

By policy design, declassification largely operates in an information environment twenty-five years in the past, making paper the dominant review format agencies must prioritize. Solutions that can assist in managing the large volumes of paper found at agencies and the National Archives already exist in the commercial world. But implementing these known solutions within government remains elusive and problematic. Funding for declassification and records management in most agencies is minimal, at best. What little funding is available supports outdated processes designed in the 1990s in response to the mandates afforded with the onset of automatic declassification. Prior to the notion of automatic declassification, declassification review occurred ad hoc and inconsistently across agencies. When adopted and implemented, these 1990s processes elevated declassification review to the program level. They have served their intended purpose - to institutionalize declassification at agencies—and presently are largely outmoded for managing electronic records. These 1990s processes will remain in place for the foreseeable future, barring resources for the development of new processes and the adoption of automated workflow tools.

In addition to the challenges of outdated paper-based processes, agencies also lack capabilities to manage the review of special media formats and legacy electronic records, including first generation born-digital records. As prioritization of records for declassification review largely depends upon records' age, the coming of "age" of electronic records review is now of serious consequence for agencies, with the added complication that no relief from paper records review appears to be in sight. Common challenges exist among agencies in managing legacy electronic records, yet there is no serious effort underway to acknowledge or describe these challenges, let alone develop a universal approach or solution.

Other common problems exist concerning electronic records beyond the issue of exponential growth and volume in need of review. Connectivity, integration and communication of systems that support declassification and records management within and between agencies is fragmented and sparse. Agencies lack universal metadata requirements and standards for managing declassification. Requirements and standards are of the utmost importance as declassification is increasingly dependent on the ability of agencies to refer their records to other agencies for equity review. Agencies must adopt and implement common solutions to these challenges across government; progress of any one agency in building a technological framework to modernize its declassification program is dependent on its ability to interact and share information with its counterparts.

Sharing information among agencies also exposes cultural challenges found in the declassification world. A common understanding and agreement for how agencies should mitigate risk does not exist. Agency practices are intolerant of risk and the consequences of not striking a balance between openness and continued secrecy in declassification review are too high for the system to sustain indefinitely, both in resources and credibility. Today's information world, including the national security structure, is increasingly dependent on transparency and open source informational content. Risk management and mitigation must be key elements of forethought in designing technical declassification capabilities, not an afterthought in response to disclosure events.

Next Steps: What Agencies Need

Technological modernization of declassification and its related functional counterpart, records management, will require leadership and resources. Agencies require both simple workflow tools and advanced content processing, analytic tools and storage/access means. Agencies should integrate declassification reviewers and records managers, organizing for success, to share best practices, manage metadata and efficiently harvest all the capabilities of information age technologies for the benefit of all system users, including policymakers and historians. Additionally, special media and first generation born-digital records demand serious consideration. A government-wide investment strategy should consider and build upon those tools in use at agencies with more modernized declassification capabilities, such as the intelligence community.

A phased adoption of sophisticated content analytic solutions should occur, beginning with an increase in the number of pilots used to test these capabilities within declassification programs. Capabilities, like those developed at the Center for Content Understanding at the Applied Research Laboratory at the University of Texas at Austin, should be implemented to a greater extent at agencies.[2] For most agencies, there is an immediate need to implement automated workflow solutions and basic search capabilities, solutions that largely exist in the commercial world that are readily available for adoption. Even while grappling with basic workflow challenges, agencies must also seriously invest in advanced content analytic tools. The sustainability of the system is dependent on agencies exploring advanced content analytic solutions while also solving immediate workflow automation challenges.

Even more importantly, the long-term transformation of the declassification system will require leadership from the White House and a commitment to funding a government-wide technology investment strategy. The PIDB will continue studying declassification technology investment at agencies with the recommendation that agencies receive the resources they need to make the records of our government accessible to future generations. Our desire is to support policymakers, while maintaining our principal responsibility of responding to the public interest in having an open and transparent government. We believe the government will only be able to achieve this goal with the adoption of technological capabilities that will modernize the security classification system to function effectively in the current digital information environment.

---

[1] Memorandum for Implementation of the Executive Order 13526, "Classified National Security Information," December 29, 2009, 75 FR 733, Document Number E9-31424. https://www.federalregister.gov/documents/2010/01/05/E9-31424/implementation-of-the-executive-order-classified-national-security-information. Accessed May 14, 2020.

[2] At the request of the CIA and the National Archives, the Center for Content Understanding at the Applied Research Laboratories at the University of Texas at Austin piloted decision- support technology for records declassification review and release. The pilots successfully yielded a Sensitive Content Identification and Marking (SCIM) tool that uses a combination of natural language processing, expert systems, machine learning and semantic knowledge representation to identify sensitive content in textual information found in classified email records. The SCIM tool is the only tool of this level of sophistication being explored for the sole purpose of aiding decision-support in classification and declassification.


PIDB