PUBLIC INTEREST
DECLASSIFICATION BOARD

Senate Select Committee on Intelligence
Hearing on Proposed Declassification Reform
Wednesday, September 9, 2020
Location: Senate Dirksen Room G-50 and via WEBEX
3:00 PM - 4:30 PM

Prepared Testimony of Congressman John F. Tierney
Member of the Public Interest Declassification Board

Good afternoon Acting Chairman Rubio, Vice Chairman Warner, and members of the Committee. Thank you for the invitation to testify on the important but often neglected issue of modernizing the Government's national security classification and declassification system. I would also like to thank the Committee staff for their assistance making it possible for me to appear before the Committee by video. I am speaking to you today as a member of the Public Interest Declassification Board, the "PIDB," and my remarks reflect the views of our members.

Congress recognized the critical importance of declassification in our democracy and in our nation's security when it created the PIDB in 2000. It recognized the role the PIDB can and should play in improving the health of our national security classification and declassification system by making recommendations for reform.

We are gratified for Senators Moran and Wyden cosponsoring and introducing "The Declassification Reform Act of 2020" as an amendment to the 2021 Intelligence Authorization Act. This proposed legislation includes many recommendations included in our most recent report to the President, *A Vision for the Digital Age: Modernization of the U.S. Classification and Declassification System.*

We are also grateful for the Congress passing and the President signing legislation last year permanently authorizing the PIDB and look forward to continuing our advocacy on the imperative to modernize today’s antiquated classification and declassification system.

Over the past 12 years, the PIDB researched and wrote five reports to the President. Each report documented challenges facing the government and recommended new policies to address them. We believe that modernization of the classification and declassification system is an imperative. It is a necessity for our national security and our democracy to operate effectively in the digital age.

Since issuing recommendations in our first report in 2008, the government has made little progress. Importantly, it has not adopted our recommendations to invest and integrate information technology into the classification and declassification processes and to modernize policies to support it. The current Executive order was last updated 11 years ago. It is now outdated and requires dramatic changes in how the government works in a fully digital environment.

We published our *Vision* report in June. It was purposefully designed as a road map for the government to overcome collective and individual agency inaction and to harness uncoordinated efforts by a few individual agencies and integrate them into a government-wide approach.

We decided a blueprint would be most useful. It would allow agencies to think creatively, cooperatively, and draw on technical expertise of all agencies. In earlier reports, many of our recommendations were not fully evaluated. Nor were alternatives or options explored. Rather, they individually focused solely on the resource and cost challenges, and simply responded, “it costs too much” and would “take resources away from our mission.” We hope the all-of-government roadmap in this report and in Senator Wyden and Senator Moran’s proposed amendment will help agencies focus on collective solutions.

Our report stressed the critical importance of sustained leadership in driving change by having a senior-level Executive Agent to oversee and implement meaningful reform. We felt that an integrated federated systems approach would ensure interoperability, allow for effective use of advanced technologies to support classification and declassification, and lead to solutions for declassifying large volumes of digital data.

Our recommendations align with the administration’s Information Technology modernization and Artificial Intelligence strategies, the President’s Management Agenda, and efforts to integrate agencies to improve performance and reduce costs.

Our recommendations address concerns identified by the IC Inspector General in its assessment of IC FOIA programs. They align with the DNI’s 2019 National Intelligence Strategy “to do things differently,” and the National Solarium’s recommendation to “reform the U.S. Government’s structure and operations for cyberspace.” These reports, like ours, stressed the need for change so our government can address 21st century mission requirements and operations. New classification and declassification policies and processes are critically important both for our democracy and for our nation’s security.

Challenges with the Current System

There is widespread agreement that the classification and declassification system is at a breaking point. It simply cannot effectively or efficiently handle the volume of digital data generated each day. It cannot handle the volume of records requiring declassification review. Policies and processes remain much the same from when they were first enacted in 1951 by President Truman in an era when secrets were created on paper and secured in combination safes.

They have not kept pace in the digital environment and do not function effectively today. Without reform, it will be far worse in the future. As I will discuss in my testimony, our national security is at risk. An important tenet of democratic government – transparency and an enlightened citizenry – is also in danger.

I have two examples to share. In our 2012 report to the President on *Transforming the Security Classification System*, we learned that one intelligence agency alone estimated it created approximately 1 petabyte of classified data every 18 months. That is equivalent to approximately 1 trillion pieces of paper. For declassification purposes, this agency also estimated that, using current manual declassification review processes, it would take two million employees one year to review this volume of information. That was *one agency 8 years ago*. The problem has now undoubtedly grown exponentially since that time.

Second, the National Archives receives all Presidential records at the conclusion of each administration. It accessioned between 1 and 2 terabytes of data from the 12-year span of the Ronald Reagan and George H. W. Bush administrations. This increased to 4 terabytes from the Clinton administration – mostly email and structured data. They received 80 terabytes from the George W. Bush administration. It accessioned an astonishing 250 terabytes of data from the Obama administration, including a complex array of structured and unstructured data.

Current declassification policies and processes cannot handle this volume of information.

Over-Classification Impacts our National Security and Will Impact Future Declassification

Just as the declassification system is about to collapse, over-classification is getting worse and is harming current government national security operations. Recently, the Senate Armed Services Committee heard from LTG

James Dickinson, the President’s nominee to lead the U.S. Space Command. He testified that over-classification was “making it more difficult for us to support the warfighter” and called for “a review of classification for collection data to ensure widest dissemination possible to the war fighter in a timely fashion.”

Over-classification not only affects operations and missions. He explained that over-classification of space information leads to costly and unnecessary duplication of space systems, reduces integration of space capabilities and training, and limits knowledge about specific space threats across U.S. operational forces.

Effective space defense relies on the collection, processing, and sharing of information that includes valuable sensor data, satellite communications, and navigation signals for a diverse set of end users. Over-classification of this information, which is strictly regulated by security controls, stymies innovation and the performance of Government engineers and contractors developing new technologies on a broad range of projects that could aid U.S. space dominance.

General John Hyten, the Vice Chairman of the Joint Staff, was equally dismayed about over-classification of information within the Defense Department, calling it “unbelievably ridiculous.” These officials, like so many others are worried about over classification’s effect on operations, costs, innovation, and the ability to partner with industry and the private sector. Like the PIDB, they also worry that over-classification limits the public’s insight into government operations and programs, especially costly ones like the defense space program.

Leaders across the DOD and the IC are struggling with the existing classification system and how it impacts their missions and costs. The costs are staggering – from an estimated $9.9 billion in FY 2007 to an estimated $18.39 billion in FY 2017. While security costs doubled during this period, declassification costs were stagnant over the same period. Collectively, agencies spent just over $102 *million* for declassification in FY 2017.

The inability of the government to make timely declassification decisions of its historical records impacts the government's ability to fulfill its statutory obligations to the American people. The State Department is required to compile and publish the official historical record of major U.S. foreign policy and national security decisions 30 years after the end of each administration in a publication called the *Foreign Relations of the United States*. According to the Historical Advisory Committee that oversees publication, this series, published since 1861, may not be viable for much longer. They report that antiquated policies and processes and the lack of resources have led to a bottle neck that is increasing and unable to handle large volumes of electronic records.

Recommendations for Reform

Crucial reforms to the system must include a tightening of definitions and greater specificity for categories requiring protection in the first place. Some measure of constraint on the system is necessary to combat over-classification. Agencies must adopt a risk-based approach to support increased and timely information sharing.

Modernization will lead to more accurate and precise classification and declassification decisions. Reforming classification practices on the front-end of the system not only support agency missions, it reduces the volume of data requiring declassification in the future.

Agencies also need to re-evaluate the needs of their customers to maximize their support. For example, the National Geospatial-Intelligence Agency (NGA) made strategic policy decisions to address these challenges with their Consolidated Security Classification Guide, called "CoNGA."

It consolidated all individual NGA classification guides into a single guide. But also required validation by an inclusive intra-agency group that meets monthly. This ensures that classification and declassification decisions align with NGA's current mission and customer needs that are digital and integrated into NGA's work processes. It uses technology to assist users in correctly applying classification decisions.

NGA is the first agency to integrate technical processes into automating classification decisions. This use of new processes and advanced technology makes classification more precise and helps users and customers.

Executive or Legislative Action to Support Necessary Policy Implementation

Modernization, interagency integration, and technology use are critical to the security of our nation. Technologies such as artificial intelligence and Machine Learning are revolutionizing operations and missions. It can and must be used to revolutionize the management of classified data. Specific tools and technology solutions exist at agencies now – although for other purposes. Additionally, policies are needed to allow agencies to share acquisition, advanced technologies, and technical expertise.

The Need for an Executive Agent

Agencies have their own classification and declassification programs. They operate independently. They are focused only on identifying and reviewing their equity information. They are duplicative. They often operate in a silo – even within their own agency as mission staff know little of classification and declassification, leading to over-classification or unauthorized disclosures that harm national security.

Many programs lack the ability to communicate securely with each other, including the National Declassification Center. This lack adds unnecessary costs and harms efficiency and effectiveness as agencies recreate and duplicate processes, repeat contactor and other costs, and utilize whatever technology they can find.

An Executive Agent is critical to reform. First, the EA has the authority to oversee implementation of new policies and processes across agencies. This coordination role includes developing specific classification and declassification guidance that can be used across agencies and make decisions more precise. The EA has authority to direct and coordinate research into advanced technology solutions, ensure its interoperability across the federated enterprise system, and has the authority to coordinate technology acquisition. The Executive Agent is responsible for progress and answerable to the President.

Why should the ODNI lead the way as the Executive Agent?

We believe that the Intelligence Community – and ODNI specifically - is strategically empowered to take on the coordination role as Executive Agent for several reasons. First, the ODNI has the experience. It successfully overcame bureaucratic roadblocks and integrated the 17 agencies and organizations that comprise the IC.

It is also a proven leader in developing, implementing, and managing new technological solutions to support missions and operations across agencies. It led the development and deployment of the Intelligence Community Information Technology Enterprise (ICITE), modeling a new information strategy across the IC under Intelligence Community Directive 121. It designed and implemented data standards, including metadata tagging, across the IC enterprise.

ODNI is a leader in overseeing and managing research in advanced information technology, artificial intelligence, and other machine-learning technologies. It leverages expertise of the Intelligence Advanced Research

Projects Agency, National Security Agency, Central Intelligence Agency, other IC agencies, and In-Q-Tel and other private sector partners.

It has experience developing and managing advanced system architectures that allow agencies to communicate with one another. The Joint Worldwide Intelligence Communication System revolutionized how agencies can securely and quickly communicate with one another, and find, use and share highly classified information. This responsibility extends outside the IC to all agencies with the need to access Top Secret information.

The DNI not only can leverage expertise across all elements of the IC and its contractors, it also has the stature necessary to both drive change and overcome bureaucratic hurdles. Should a challenge arise, the DNI can contact her/his counterpart to resolve the challenge, ask for additional technical or other expertise to problem-solve, direct an agency to lead a task, and coordinate standards and requirements.

Lastly, its 2019 National Intelligence Strategy recognizes the DNI's leadership role in getting the government "to do things differently" by "increasing integration and coordination," "bolstering innovation," and "increasing transparency." We felt the ODNI was the clear choice to serve as the Executive Agent.

The ODNI already coordinates the implementation of technology in protecting and sharing sensitive government information across Federal agencies— including beyond the Intelligence Community. For example:

- During the current public health emergency, ODNI policies continue to guide the electronic collection and sharing of classified information between the IC and civilian agencies, including the Office of the Assistant Secretary for Preparedness and Response in the Department of Health and Human Services;

- The ODNI developed the first Intelligence Community Environment Data Strategy. It provides a framework for applying advanced analytics and big data techniques to store, process, exploit, and manage highly classified information while protecting sensitive sources and methods. It also coordinates the implementation of this framework across the IC between the various Chief Data Officers responsible for data policy, and the various Chief Information Officers responsible for technology acquisition. It has the structure and staff in place to implement and adapt this framework outside the IC.

- The ODNI's role in integrating and sharing intelligence collection and analysis through the Intelligence Community Information Technology Enterprise (ICITE). It establishes the infrastructure for the expanding application of Artificial Intelligence, Machine Learning, Automation, and other information technologies to manage information across the IC.

- The ODNI's role in overseeing the protection of sensitive sources and methods. This is a critical concern of IC agencies. However, information received from intelligence sources and methods is shared outside of the IC. The ODNI already manages and establishes policies and processes for the dissemination of this information across government.

Unfortunately, the successful and increasingly routine modernization of information sharing and information security focuses almost exclusively on supporting current Government missions and operations. There has been little thought or action in how to apply technology and integrate it into modernizing the classification and declassification system.

The PIDB believes that advances by the ODNI in establishing a common IT architecture can also provide opportunities to gain efficiencies, better support missions, and increase cost savings by expanding the common IT infrastructure, processes, and data strategy already in place to improve classification and declassification.

A failure of leadership and the will to apply these advances across the Executive Branch to integrate classification and declassification within the existing IC infrastructure for managing electronic information can only result in:

- redundant collection and analysis, and the continuing failure to exploit legacy intelligence in future operations against emerging national security threats;

- new backlogs in the declassification of electronic information assets that compound the initial expense of collection and analysis with excessive storage and handling costs, and which stifle access critical to effective policymaking and public discussion;

- inhibit necessary public discourse without the application of proven technological solutions.

Concluding Remarks

Our Board has now authored five reports to the President offering recommendations and possible solutions to this challenge. However, our recommendations have not led to an overhaul of the system. They have yet not led to any coordinated government effort to radically rethink what classification and declassification mean in the digital age.

During this time, government declassification programs have remained duplicative and stove-piped, seemingly ensconced in their own bubbles. Each agency performs the same function. Each day hundreds of reviewers put eyes on page after page, with multiple reviewers reading the same pages. Decisions can be haphazard and even contradictory. Guidance, if easily available, is general and mistakes are made - hindering democratic transparency, adding additional unnecessary safeguarding costs, and compromising real secrets. Technology usage is illusory.

We are at the precipice. The declassification system can no longer keep pace with the volume of paper records created 25 years ago. The growth of digital data will cause it to collapse without radical change.

The impact of a failure to reform the declassification and classification system will be felt widely - on our democracy and on our national security.

Our Board remains hopeful that change is coming. The President signed Senate Bill 1790 last year reauthorizing our Board. It also required the Department of Defense to report to the Congress on what it is doing to reduce declassification backlogs and modernize its declassification processes. The report requires the Secretary of Defense to provide Congress with its plan for adopting and integrating advanced technologies in its declassification processes. Although we have not had any communication with the Department of Defense since this requirement was enacted, we understand that the pandemic has delayed its preparation and completion until later this Fall.

We support Senator Moran’s and Senator Wyden’s recently proposed legislation to modernize declassification. It is another important step forward.

There is unanimity within the government and with all stakeholders that this system is outdated and will not work in the digital age. Listening to representatives from the ODNI testifying today – agreeing that the system is outdated – is a step forward. Recognizing that there is a problem in the first place is always the first step in finding a solution.

This hearing – dedicated to the problem of addressing outdated declassification policies and practices – is a step forward.

There is agreement that entirely new policies and processes are required.

There is agreement that new processes must be developed and incorporate the use advanced technologies. And that new policies must facilitate the use of these technologies.

These are all important steps for the government to build on. The government is already modernizing information technology policies and practices. It is reforming acquisition policies and practices for efficiency and reduced costs. It is integrating the use of advanced technology across agencies to address mission imperatives.

Adopting the recommendations in our *Vision* report – either within the Executive branch or through legislation – are the next steps. Appointing the DNI as the Executive Agent will bring needed experience and expertise. It will facilitate development of a federated systems approach. It will facilitate modernization and the integration of advanced information technology into new classification and declassification processes.

Let me express my appreciation to the Committee for addressing this esoteric yet critically important topic. Modernizing the classification and declassification system <u>is</u> important for our 21st century national security and it <u>is</u> important for transparency and our democracy.

The time for action is now. The government must move beyond simply saying "no" or saying, "it is too costly" or saying, "some other agency should be responsible." Instead, the roadmap in our report offers opportunities for reform. It offers possible solutions the government to engage with stakeholders to truly address this challenge, identify solutions, and implement them.

Of course, if requested, we, the members of the PIDB stand ready to assist the government.

Thank you for your interest and your support. I look forward to answering your questions and continuing this discussion.