Executive Summary of the Report to the President from the Public Interest Declassification Board on Transforming the Security Classification System

EXECUTIVE SUMMARY

A democratic society is grounded in the informed participation of the citizenry, and their informed participation requires access to Government information. An open record of official decisions is essential to educate and inform the public and enable it to assess the policies of its elected leaders. If officials are to be accountable for their actions and decisions, secrecy must be kept to the minimum required to meet legitimate national security considerations. To maintain democratic values, Government must act to ensure openness and should have to justify any resort to secrecy. Better access to Government records and internal history will help both policymakers and the American public meet their mutual responsibilities to address national security and foreign policy challenges consistent with democratic values.

As requested by the President, the Public Interest Declassification Board (the Board) researched and studied the security classification system in cooperation with the National Security Advisor to design a fundamental transformation of the security classification system.[i] The Board sought to understand how classified records of every level of sensitivity are managed and how different users influence classification and declassification decisions at the front-end and the back-end of the system. The Board met extensively with stakeholders inside and outside of government during its study: senior government officials, Executive departments and agencies (agencies), distinguished civil servants, the Congress, leading technologists, experts from public interest, civil society and transparency groups, historians, classifiers, declassifiers, and archival researchers. Its research led the Board to understand the challenges the system presents to all users and to solicit suggestions and ideas for its transformation. The findings of the Board are conclusive; present practices for classification and declassification of national security information are outmoded, unsustainable and keep too much information from the public. The prevalence of electronic records has made the current paper-based system of classification and declassification unworkable. Use of advanced information technology is crucial to achieving increases in efficiency and better balancing information security with government openness. However, there is little evidence that Executive departments and agencies (agencies) are employing or developing the technologies needed to meet these objectives.

Reforms are essential if we expect to manage the increased volume of records, share critical information among agencies and live within available resources. Essential to such reforms must be improved integration of classification and declassification programs and better resolution of the inherent tension between keeping secrets and ensuring the openness required for an accurate historical record.

This report describes the difficulties—both technical and cultural—we face in reforming the system and recommends practicable steps to overcome them and effect reform. The Board understands the many challenges facing agencies in today's resource-constrained environment. Nonetheless, the measures in this report are critical to modernize a security classification program capable of protecting our nation and supporting fundamental democratic values and transparency. The Board recognizes there is disagreement among stakeholders with many of the recommendations in its report. Modernization is difficult and bureaucracies' natural tendency is to maintain the status quo. These recommendations will succeed only with a determined implementation strategy and vigorous oversight backed by the President. The Board believes it will require a White House-led steering committee to drive reform, led by a chair who is carefully selected and appointed with specific authorities granted by the President. A White House-led Security Classification Reform Steering Committee, appointed by and accountable to the President, should manage the implementation of the reforms required to transform current classification and declassification guidance and practice.[ii]

Transforming the Classification System

After extensive research and discussions with stakeholders in and outside Government, the Board has concluded that the current classification system is fraught with problems. In its mission to support national security, it keeps too many secrets, and keeps them too long; it is overly complex; it obstructs desirable information sharing inside of government and with the public. There are many explanations for over-classification: most classification occurs by rote; criteria and agency guidance have not kept pace with the information explosion; and despite the Presidential order to refrain from unwarranted classification, a culture persists that defaults to the avoidance of risk rather than its proper management.

To address the concerns of excessive classification under present practice, the Board recommends:

- Classification should be simplified and rationalized by placing national security information in only two categories. This would align with the actual two-tiered practices existing throughout government, regarding security clearance investigations, physical safeguarding, and information systems domains. Top Secret would remain the Higher-Level category, retaining its current, high level of protection. All other classified information would be categorized at a Lower-Level, which would follow standards for a lower level of protection. Both categories would include compartmented and special access information, as they do today. Newly established criteria for classifying information in the two tiers would identify the needed levels of protection against disclosure of the information. Using identifiable risk as the basis for classification criteria should help in deciding if classification is warranted and, if so, at what level and duration.
- Classified national security information in the two tiered model would continue to be subject to declassification in accordance with the requirements of Executive Order 13526, "Classified National Security Information".[iii] The two tiers should be defined and distinguished by the level of identifiable protection needed to safeguard and share information appropriately, and these protection levels would determine whether classification is warranted, at what level, and for how long. Classification guidance would clearly define levels of protection by identifying a specific consequence of release of the classified information and the potential harm to the national security of limiting the sharing of the information. The difficulty of applying the current concept of presumed "damage" during derivative classification would be replaced by a more concrete application of level of protection necessary for sharing and protecting. This change in guidance would reflect how classification is actually practiced by derivative classifiers—deciding how much protection is needed based on the sensitivity of the information to both protect and share appropriately. Determining a level of protection to facilitate or impede dissemination is more prescriptive in practice and would assist classifiers in making more accurate classification decisions. Applying this risk management practice by identifying the level of protection needed based on the sensitivity of the information, rather than potential damage if disclosed, should allow users to classify information at the lowest level of protection or to keep the information unclassified. Specific protections accorded intelligence and non-intelligence sources and methods should also be better-defined and -distinguished.
- The Board recognizes that the adoption of a two-tiered model will pose greater challenges for those agencies whose internal practices are more dependent upon current distinctions between Secret and Confidential.

- Classified information that is operational or based on a specific date or event should be automatically declassified without additional review or exemption when that operation or event passes. The records containing this perishable information should be marked as classified "Short-term" (or similar term) at the time of creation.
- In order to effect the cultural shift implicit in these recommendations, guidance should assume that classification decisions are made in good faith and should afford a 'safe harbor' for classifiers who adhere to proper risk management practices and, when unsure, decide not to classify. Classification training should address the culture bias that favors classification, and often over-classification, through coordinated, consistent education that underscores the responsibility to not classify in the presence of doubt.

As discussed in the technology section of this report, available technologies, such as context accumulation, predictive analytics and artificial intelligence, should be piloted to study their effectiveness on helping implement these recommendations and to engage users and garner their trust in a new system.

Transforming the Declassification System

Declassification is a complex and time-consuming process, typically performed in a culture of caution without much attention to efficiency and risk management. Sequential referral of classified records for review by each agency that claims an "equity" in the record takes a great deal of time.[iv] Agencies are reluctant to share their declassification guidelines, impeding efficiency that could be realized from greater interagency coordination and collaboration. Because declassification is not seen as a way to serve the national security mission, the public's right to know what its government does is not well-served.

The problem is growing. Agencies are currently creating petabytes of classified information annually, which quickly outpaces the amount of information the Government has declassified in total in the previous seventeen years since Executive Order 12958 established the policy of automatic declassification for 25 year old records.[v] Without dramatic improvement in the declassification process, the rate at which classified records are being created will drive an exponential growth in the archival backlog of classified records awaiting declassification, and public access to the nation's history will deteriorate further.

To address this serious concern, the Board recommends streamlining the declassification process as follows:

- A process should be implemented for the systematic declassification review of historical Formerly Restricted Data (FRD) information. The Departments of Energy and Defense may choose to convert historical FRD information either to Restricted Data information or to classified national security information.[vi] FRD information concerns the military utilization of nuclear weapons, including storage locations and stockpile information and often dates from the end of World War II through the height of the Cold

New Classification Category	Old Classification Category	Level of Protection	
Higher-Level "Top Secret"	Top Secret	Higher level of protection	Includes compartmented and special access information
Lower-Level	Confidential and Secret	Lower level of protection	

War. Although often no longer sensitive or current, this type of FRD information is of high interest to researchers yet remains largely unavailable to the public, because there is no process for systematically reviewing it for declassification and release under the terms of the Executive Order for national security information.

- Strengthen the National Declassification Center (NDC) to establish a more coordinated government-wide declassification system.
    - Executive Order 13526 should be revised to eliminate the additional three years now authorized to process multiple agency equities in all archival records (including those outside the NDC).
    - The declassification system should manage risk and better balance resource-intensive agency reviews with the democratic value of timely public release. Rules that govern declassification, including those concerning historical nuclear information, should tolerate greater risk.[vii]
    - Streamlined archival processing should expedite public release of declassified records, with such records automatically transferred to the National Archives and Records Administration (National Archives).[viii]
    - Public representatives, including experts from the Government Openness advocacy community, should be added to the interagency NDC Advisory Panel (NAP) advising the NDC Director.[ix]
- Immediately require agencies to share declassification guidance and training and prioritize the review of historically significant records and ensure timely transfer to the National Archives.
- Streamline activities of both the NDC and agencies to complement the modernization initiatives directed by the President in his Memorandum on Managing Government Records.[x]
- Classification and declassification program staffs should collaborate with agency historians and records officers to ensure that historically significant information is identified as early as possible in its "life" and then set aside for historical review and preserved for the long-term. Agency histories, both classified and unclassified, should serve policymakers and operational leaders with "lessons learned" as well as contributing to the historical record. Agency history programs should be promoted across Government and aligned in "centers" that bring declassification reviewers and historians together. Classified histories should be reviewed at a specified interval for declassification and release to the public.
- Pilot projects should be identified to develop best practices and design a more streamlined system.

Using Technology to Aid Classification and Declassification

Classification and declassification are not keeping pace with the myriad of challenges facing the system: digital information creation, access for cleared persons, existing backlogs of paper holdings awaiting declassification review, long-term storage requirements, or the rights of a democratic society to as much information as possible about its Government. Available technologies are rarely used to meet current needs; neither are agencies preparing to use these technologies to handle the enormous volume of digital records. As a result, the Government is currently unable to preserve or provide access to a great many important records.

The challenge can be met only with determined efforts to modernize classification and declassification by employing existing technologies and developing new tools. Agencies should collaborate on policy, share technologies, promote best practices and develop common standards. Metadata are especially critical to future high-speed data manipulation in the digital era. Promising new technologies should be tested through a series of pilot projects, beginning with a declassification project at the NDC; once proven, they can be deployed at multiple agencies and then expanded to include pilot projects for classification. The ultimate goal of these pilots is to discover, develop and deploy technology that will:

- Automate and streamline classification and declassification processes, and ensure integration with electronic records management systems.

- Provide tools for preservation, search, storage, scalability, review for access, and security application.
- Address cyber security concerns, especially when integrating open source information into classified systems.
- Standardize metadata generation and tagging, creating a government-wide metadata registry. Lessons learned from the intelligence community will be helpful here.
- Accommodate complex volumes of data (e.g. email, non-structured data, and video teleconferencing information).
- Advance government-wide information management practices by supporting the President's Memorandum on Managing Government Records.

The President should hold the Steering Committee accountable for ensuring the interagency collaboration needed to employ existing technologies and develop new methods to modernize classification and declassification.

ENDNOTES *for* EXECUTIVE SUMMARY

[i] Memorandum for Implementation of the Executive Order 13526, "Classified National Security Information," December 29, 2009, 75 FR 733, Document Number E9-31424.

[ii] Modeled on the Senior Information Sharing and Safeguarding Steering Committee, Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," 76 FR 63811, Document Number 2011-26729. The Public Interest Declassification Board would be available to assist this committee.

[iii] Executive Order 13526, "Classified National Security Information," 75 FR 68675, Document Number 2010-28360.

[iv] An equity is information that was originated, created by, classified by, or concerns the activities of a specific government agency or organization and, as owners of the information, only they can declassify it. Records that contain multiple agency "equities" must be referred to those agencies for declassification review. Sources: 32 C.F.R. Parts 2001 and 2003 Classified National Security Information; Final Rule, section 2001. 92(g), 75 FR 37279, Document Number 2010-15443 and The U.S. Department of Justice, Office of Information and Privacy (http://www.justice.gov/open/declassification/).

[v] One intelligence agency estimates that one terabyte of data is equivalent to approximately 112 million pages of information, making one petabyte of data equivalent to approximately 1.2 trillion pages of information. The Government declassified 1.27 billion pages of information between FY 1995 and 2011 according to figures from the FY 2011 Annual Report to the President from the Information Security Oversight Office. (*http://www.archives.gov/isoo/reports/2011-annual-report.pdf*). Executive Order 12958, "Classified National Security Information" is a predecessor order to today's Executive Order 13526. See Endnote 2.

[vi] Contemplation of recommendations regarding RD and FRD should include determination if legislative changes are needed.

[vii] Agencies have adopted conservative "no risk" practices when reviewing records for declassification. Agencies use this "no risk" practice most notably when implementing the requirements of the National Defense Authorization Acts for Fiscal Year 1999 and 2000 (Public Laws 105-261 and 106-65 respectively), which relate to RD/FRD.

[viii] Currently, many transfers of declassified records to the National Archives are hindered by outdated scheduling requirements, making declassified records unavailable to users.

[ix] The NDC Director is currently advised by an interagency NDC Advisory Panel (NAP) and assisted by an inter-agency Program Management Team (PMT). The NAP examines current declassification review processes throughout government. It consists of senior managers from the Departments of State, Defense, and Energy as well as the Central Intelligence Agency, Director of National Intelligence, the Information Security Oversight Office, and the National Archives.

[x] Managing Government Records, Memorandum for the Heads of Executive Departments and Agencies, A Presidential Document by the Executive Office of the President on 11/28/2011, 76 FR 75423, Document Number 2011-31096. The Office of Management and Budget issued *M-12-18, Managing Government Records Directive* on August 24, 2012. This Directive creates a robust records management framework that complies with statutes and regulations to achieve the benefits outlined in the Presidential Memorandum. This Directive was informed by agency reports submitted pursuant to Sec. 2 (b) of the Presidential Memorandum and feedback from consultations with agencies, interagency groups, and public stakeholders.