BRENNAN CENTER FOR JUSTICE

REDUCING OVERCLASSIFICATION THROUGH ACCOUNTABILITY

Elizabeth Goitein and David M. Shapiro

Brennan Center for Justice *at New York University School of Law*

ABOUT THE BRENNAN CENTER FOR JUSTICE

The Brennan Center for Justice at New York University School of Law is a non-partisan public policy and law institute that focuses on the fundamental issues of democracy and justice. Our work ranges from voting rights to campaign finance reform, from racial justice in criminal law to presidential power in the fight against terrorism. A singular institution—part think tank, part public interest law firm, part advocacy group—the Brennan Center combines scholarship, legislative and legal advocacy, and communications to win meaningful, measurable change in the public sector.

ABOUT THE BRENNAN CENTER'S LIBERTY AND NATIONAL SECURITY PROGRAM

The Liberty and National Security Program was established in 2004 to advance effective national security policies that promote constitutional values and the rule of law. To that end, the Program seeks to develop and deepen a public consensus about the relevance of liberty and the rule of law in national security policy, to advance institutional reforms reflecting that consensus, to advocate for appropriate restraints on—and accountability for—the exercise of executive power, and to stand as a bulwark against the erosion of basic freedoms.

ABOUT THE AUTHORS

Elizabeth Goitein co-directs the Brennan Center for Justice's Liberty and National Security Program, which seeks to advance effective national security policies that respect constitutional values and the rule of law. Before coming to the Brennan Center, Ms. Goitein served as counsel to Senator Feingold, Chairman of the Constitution Subcommittee of the Senate Judiciary Committee. As counsel to Senator Feingold, Ms. Goitein handled a variety of liberty and national security matters, with a particular focus on government secrecy and privacy rights. She also worked on matters involving immigration, juvenile justice, sentencing, prisoner re-entry, and First Amendment issues. Previously, Ms. Goitein was a trial attorney in the Federal Programs Branch of the Civil Division of the Department of Justice. Ms. Goitein graduated from the Yale Law School in 1998 and clerked for the Honorable Michael Daly Hawkins on the U.S. Court of Appeals for the Ninth Circuit.

Ms. Goitein's writing has been featured in major newspapers including *The Washington Post, The Boston Globe, The San Francisco Chronicle,* and *The Philadelphia Inquirer,* as well as prominent outlets such as *Roll Call, The National Law Journal,* and *The Huffington Post.* She has appeared on national television and radio shows including the *PBS NewsHour* and National Public Radio's *On the Media.*

David M. Shapiro worked as Counsel in the Brennan Center's Liberty and National Security Program, focusing on classification, government secrecy, and isolation conditions imposed on U.S. prisoners due to supposed connections to terrorist groups. Mr. Shapiro is currently a Staff Attorney at the ACLU's National Prison Project, where he litigates cases and engages in advocacy regarding prison and detention conditions, including immigration detention, access to information about prison conditions, the right of prisoners to communicate with the outside world and to practice religion, and the freedom from arbitrary body cavity searches. Mr. Shapiro worked as an associate at Davis Wright Tremaine LLP, where he litigated First Amendment cases in federal trial and appellate courts, and served as a law clerk to Judge Edward R. Becker, United States Court of Appeals for the Third Circuit. Mr. Shapiro is a graduate of Harvard College and Yale Law School and studied in Moscow, Russia as a Fulbright Scholar.

ACKNOWLEDGEMENTS

The authors would like to thank the Brennan Center's Emily Berman, Deborah Francois, Erik Opsal, Faiza Patel, Jeanine Plant-Chirlin, Sidney Rosdeitcher, Michael Waldman, and Jennifer Weiss-Wolf for their invaluable input and support; Kyle Alagood, Molly Alarcon, Stephanie Friedberg, and Kelsey Linebaugh for their dedicated research assistance; and the Brennan Center's Chief Counsel, Fritz Schwarz, who shared the insights and expertise stemming from a lifetime of study on the subject of government secrecy, including his recent work on a forthcoming book. In addition, the authors benefited greatly from conversations and correspondence with Amy Bennett, Thomas Blanton, William J. Bosanko, Spike Bowman, Danielle Brian, Morris Davis, Louis Fisher, Sharon Bradford Franklin, Mike German, George Jameson, Ronald Marks, Patrice McDermott, Joseph Pfeifer, John Powers, Suzanne Spaulding, Serrin Turner, Matthew Waxman, and a number of current and former government officials who asked not to be identified. The authors extend special thanks to Steven Aftergood and J. William Leonard, who generously shared their time and considerable expertise at every stage of this project. The views expressed in this report are solely the responsibility of the Brennan Center.

The Brennan Center is grateful to The Atlantic Philanthropies, CS Fund / Warsh-Mott Legacy, Democracy Alliance Partners, The Herb Block Foundation, Open Society Foundations, and William C. Bullitt Foundation for their generous support of our Liberty and National Security Program.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The authority to classify documents exists to protect information that could threaten national security if it got into the wrong hands. It is one of the most important tools our government has to keep us safe. But many secrets "protected" by the classification system pose no danger to the nation's safety.

On the contrary, needless classification—"overclassification"[1]—jeopardizes national security. Excessive secrecy prevents federal agencies from sharing information internally, with other agencies, and with state and local law enforcement, making it more difficult to draw connections and anticipate threats. The 9/11 Commission found that the failure to share information contributed to intelligence gaps in the months before the September 11, 2001, attacks, cautioning that "[c]urrent security requirements nurture overclassification and excessive compartmentation of information among agencies."[2]

Overclassification also corrodes democratic government. Secret programs stifled public debate on the decisions that shaped our response to the September 11 attacks. Should the military and CIA have used torture to extract information from detainees in secret overseas prisons and at Guantánamo Bay? Should the National Security Agency have eavesdropped on Americans' telephone calls without warrants? Even leaving aside the legality of these measures, whether to use torture or to forego the use of warrants are questions that, in a democracy, properly belong in the public sphere. Classification forced the nation to rely on leaked information to debate these questions, and to do so well after torture and warrantless surveillance programs were in place.

Overclassification is rampant, and nearly everyone who works with classified information recognizes the problem. In 1993, Senator John Kerry, who reviewed classified documents while chairing the Senate Select Committee on POW/MIA Affairs, commented, "I do not think more than a hundred, or a couple of hundred, pages of the thousands of [classified] documents we looked at had any current classification importance…."[3] And two years later, Donald Rumsfeld, while noting that disclosure of truly sensitive information can put lives at risk, acknowledged, "I have long believed that too much material is classified across the federal government as a general rule."[4]

Government statistics bear out these assessments. When a member of the public asks an agency to review particular records for declassification (through a process called "mandatory declassification review"), 92 percent of the time the agency determines that at least some of the requested records need not remain classified.[5] But the number of documents reviewed through this process pales in comparison to the universe of documents that, though they may not require classification, remain unreviewed—and thus classified—for many years.

Past and present instances of overclassification include the following notable examples:

- In 1947, an Atomic Energy Commission official issued a memo on nuclear radiation experiments that the government conducted on human beings. The memo instructed, "[N]o document [shall] be released which refers to experiments with humans and might have [an] adverse effect on public opinion or result in legal suits. Documents covering such work . . . should be classified 'secret.'"[6]

- Responding to a Freedom of Information Act request by the National Security Archive, the Defense Intelligence Agency in 2004 blacked out portions of a biographical sketch of General Augusto Pinochet, even though the Clinton administration had already declassified the document. Redacted portions revealed that Pinochet "[d]rinks scotch and pisco sours; smokes cigarettes; likes parties. Sports interests are fencing, boxing and horseback riding."[7]

- In response to a Freedom of Information Act request, the Department of Defense in 2010 refused to declassify 60-year-old documents about a program called "Poodle Blanket," which planned for a potential conflict with the Soviets over West Berlin.[8]

A major theme of this report—and a source of frustration to those who have studied the classification system—is the persistent gap between written regulation and actual practice. Chief executives since Franklin Delano Roosevelt have issued executive orders on classification. Classification authority emanates primarily from these orders, which have long purported to impose common-sense limits, such as a ban on using classification to conceal embarrassing information about government officials. And the current order—Executive Order 13,526, which President Obama issued in December 2009—includes further limits, such as a requirement that records not be classified if significant doubt exists about the need for secrecy.[9] In practice, however, such limits too often fall by the wayside. As a Senate Commission chaired by Daniel Patrick Moynihan found, "Any policy, including on classification and declassification, is only as good as its implementation."[10]

This report focuses on improved implementation, i.e., how to make sure that classifiers comply with existing criteria for classifying documents. It does not address ways in which the classification system could be improved by changing those criteria, such as revising agency classification guides—which govern many classification decisions—to eliminate classification categories that are outdated, unnecessary, or imprecise;[11] requiring classifiers to weigh national security risks against the public interest in disclosure;[12] or amending the National Security Act of 1947 to clarify that "intelligence sources and methods" may be classified only if their disclosure would harm national security.[13] Measures to improve the substantive criteria for classification will form a critical piece of any successful reform effort, and their omission from this report should not be taken as an assessment of their relative importance. But the widespread failure of classifiers to comply with existing rules suggests that changing them will have little effect until we understand and address the persistent gap between rules and reality.

This report concludes that the primary source of the "implementation gap" is the skewed incentive structure underlying the current system—a structure that all but guarantees overclassification will occur. Numerous incentives push powerfully in the direction of classification, including the culture of secrecy that pervades some government agencies; the desire to conceal information that would reveal governmental misconduct or incompetence; the relative ease with which executive officials can implement policy when involvement by other officials, members of Congress, and the public is limited; the pressure to err on the side of classification rather than risk official sanctions or public condemnation for revealing sensitive information; and the simple press of business, which discourages giving thoughtful consideration to classification decisions. By contrast, there are essentially no incentives to refrain from or challenge improper classification. After all, classification is an easy exercise that can be

accomplished with little effort or reflection; those who classify documents improperly are rarely if ever held accountable—indeed, there is no reliable mechanism in place to identify them; classifiers receive insufficient training in the limits of their authority; and those who have access to classified information are neither encouraged to challenge improper classification decisions nor rewarded for doing so.

In order to succeed, any effort to reduce overclassification must address this problem of skewed incentives. The final chapter of this report sets forth a reform proposal that would rebalance existing incentives, primarily by introducing accountability into the classification system. The proposal consists of six main parts:

- When classifying documents, officials would be required to complete short electronic forms in which they would provide explanations for their classification decisions.

- In each agency with classification authority, the Office of the Inspector General would conduct "spot audits" of classifiers, identifying those who exhibit serious tendencies to overclassify and subjecting them to periodic follow-up audits.

- Successive unsatisfactory audit results would result in mandatory escalating consequences for the individual classifier, agency management, and the agency itself.

- Agencies would be required to spend at least eight percent of their security classification budgets on training and to obtain approval of their training materials from the government office that oversees classification.

- Derivative classifiers (those who carry forward classification decisions made by others) would be "held harmless" if they failed to classify information whose status was ambiguous.

- Agencies would establish procedures to allow authorized holders of classified information to challenge classification decisions anonymously, and those who brought successful challenges would be given small cash awards.

We recommend that this proposal be implemented as a pilot project at one or more agencies. This could be accomplished largely if not exclusively through executive order and implementing regulation. The results of the project should be closely tracked and evaluated to assess both its benefits and its costs. If the proposal yields the expected dividends, it could be expanded through legislation. One thing is certain: the status quo is untenable. The classification system must be reformed if we are to preserve the critical role that transparent government plays in a functioning democracy.

I. THE PROBLEM OF OVERCLASSIFICATION

Overclassification is a perennial problem, and one that causes serious harm. This chapter discusses the persistence of overclassification and the damage that needless secrecy inflicts on national security, democratic government, and the public fisc.

A. History

Overclassification is as old as classification itself. A 1940 executive order on classification by President Franklin Delano Roosevelt marked the beginning of the modern classification regime,[14] and each of the multiple government studies to address the issue since then has reported widespread overclassification.

Coolidge Committee: In 1956, the Defense Department Committee on Classified Information, convened by Secretary of Defense Charles Wilson to study classification at the Department of Defense and chaired by Assistant Secretary Charles Coolidge,[15] warned that "overclassification has reached serious proportions."[16]

Wright Commission: Responding to a congressional mandate, the Commission on Government Security, chaired by Loyd Wright, former President of the American Bar Association, prepared a comprehensive review of government security in 1957.[17] The Commission's Report, which occupied nearly eight hundred pages and required eighteen months to complete, noted that "[i]n the course of its studies, the Commission has been furnished with information classified as 'confidential' which could have been so classified only by the widest stretch of the imagination."[18]

Moss Subcommittee: In 1958, the House Special Government Information Subcommittee, under Chairman John E. Moss, issued a report on secrecy within the Department of Defense. The report found "innumerable specific instances" of unnecessary secrecy "which ranged from the amusing to the arrogant."[19]

Seitz Task Force: Chaired by Frederick Seitz, former head of the National Academy of Sciences, the Defense Science Board Task Force on Secrecy focused on the effects of classification on scientific progress and reported its findings to the Chairman of the Defense Science Board in 1970. The Task Force reported that "the volume of scientific and technical information that is classified could profitably be decreased by perhaps as much as 90 percent …."[20]

Stilwell Commission: Following the arrest of Navy members charged with espionage, Defense Secretary Caspar Weinberger established the Commission to Review DoD [Department of Defense] Security Policy and Practices, chaired by General Richard Stilwell. The Stilwell Commission focused on "systemic vulnerabilities or weaknesses in DoD security policies."[21] In 1985, the Stilwell Commission reported that, at the Department of Defense, "too much information appears to be classified."[22]

Joint Security Commission: Following the end of the Cold War, Defense Secretary William Perry and CIA Director R. James Woolsey established the Joint Security Commission to "develop a new approach

Government officials of all political stripes have criticized the classification of documents that pose no risk to national security, giving startling estimates of the problem's scope.

to security."[23] In 1994, the Commission found that "the classification system … has grown out of control. More information is being classified and for extended periods of time."[24]

Moynihan Commission: In 1997, the Commission on Protecting and Reducing Government Secrecy, a bipartisan congressional body chaired by Senator Daniel Patrick Moynihan, issued a comprehensive report on the classification regime. The report found that "[t]he classification system … is used too often to deny the public an understanding of the policymaking process."[25]

Despite the sobering findings of these various bodies, the recommendations they generated were almost never adopted. Thus, according to a leading expert on classification, although "generations of critics have risen to attack, bemoan, lampoon, and correct the excesses of government secrecy," they have rarely "had a measurable and constructive impact."[26]

Indeed, some fifty years after the Coolidge Committee's report, the 9/11 Commission highlighted the same problem: "Current security requirements nurture overclassification and excessive compartmentation of information among agencies."[27] This overclassification and compartmentation may have come at a high price. According to the 9/11 Commission, these problems inhibited information sharing, making it more difficult for the government to piece together disparate items of information and anticipate the September 11 attacks.[28]

In recent years, government officials of all political stripes have criticized the classification of documents that pose no risk to national security, giving startling estimates of the problem's scope. Rodney B. McDaniel, National Security Council Executive Secretary under President Reagan, estimated that only ten percent of classification was for "legitimate protection of secrets."[29] A top-ranking Department of Defense official in the George W. Bush administration estimated that overclassification stood at 50 percent.[30] While not putting a number on the problem, former CIA Director Porter Goss admitted, "[W]e overclassify very badly. There's a lot of gratuitous classification going on . . . ."[31]

Stark examples of overclassification have occurred throughout the history of the modern classification regime. Some border on the absurd, while others represent violations of the public trust:

- A World War II-era report by the Navy titled "Shark Attacks on Human Beings" remained classified until 1958, when the Moss Subcommittee inquired whether the report warranted classification. The report "detailed 69 cases of shark attacks upon human beings; 55 of the attacks occurred between 1907 and 1940 and at least 5 of the remaining 14 attacks were covered in newspaper stories published prior to the report. The classified document also included an article entitled 'The Shark Situation in the Waters About New York,' taken from the Brooklyn Museum Quarterly of 1916."[32]

- In *New York Times Co. v. United States*,[33] the Nixon administration argued in the Supreme Court for a prior restraint against publication of the "Pentagon Papers"—government documents regarding relations between the United States and Vietnam. Before oral argument, Solicitor General Erwin Griswold reviewed the items that the Department of Defense, State Department, and National Security Agency wanted to keep secret and "quickly came to the conclusion that most of them presented no serious threat to national security."[34] Ultimately, due to Griswold's objections, the government maintained its claim of secrecy with respect to only a fraction of these items in court.

- In its 1997 report, the Moynihan Commission noted that a memo on "an upcoming 'family day' in which family members could visit [an] agency was classified Confidential because the person who signed the memorandum was under cover. By simply omitting the name of that individual, the memo would have been unclassified."[35]

- During the Clinton administration, the CIA released the government's annual intelligence budget for fiscal years 1997 and 1998, but then asserted that historical budget figures from decades earlier—going back as far as 1947—had to remain secret. [36]

- A 2006 cable from a U.S. diplomat described a wedding he attended in Russia's Republic of Dagestan. The paragraph describing a typical Dagestani wedding was classified as "Confidential," meaning that its release "reasonably could be expected to cause damage to the national security."[37] The paragraph included the following classified observations:

  > Dagestani weddings . . . take place in discrete parts over three days. On the first day the groom's family and the bride's family simultaneously hold separate receptions. . . . The next day, the groom's parents hold another reception, this time for the bride's family and friends, who can "inspect" the family they have given their daughter to. On the third day, the bride's family holds a reception for the groom's parents and family.[38]

- In the 1960s, the FBI wiretapped Dr. Martin Luther King, Jr.'s telephone. Information about this activity was classified "Top Secret," meaning that its disclosure "reasonably could be expected to cause exceptionally grave damage to the national security,"[39] even though its sole purpose, in the FBI's own words, was to gain information about King's personal life that could be used to "completely discredit [him] as the leader of the Negro people."[40]

- The Air Force Office of Special Investigations classified a paper on "Espionage in the Air Force Since World War II," submitted by a master's degree candidate at the Defense Intelligence College. One page, marked as "Secret," contained nothing but the following quote from *The Light of Day*, a spy novel by Erick Ambler: "I think that if I were asked to single out one specific group of men, one category, as being the most suspicious, unreasonable, petty, inhuman, sadistic, double-crossing set of bastards in any language, I would say without hesitation: 'The people who run counterespionage departments.'"[41]

B. The Costs of Overclassification

The appropriate classification of information is a key way in which the government protects and promotes public safety. If information that merits classification is released, whether by mistake or through leaks, the cost can be extraordinarily high. In extreme cases, lives may be endangered. This fact is well understood; indeed, it forms the underlying justification for the classification system.

The costs of overclassification are less evident, but they can be equally grave. Overclassification causes three principal harms. First, it creates threats to national security by preventing government officials from sharing information with each other and by fostering leaks. Second, it keeps voters and (at times) Congress uninformed about government conduct, thus impairing democratic decision making and increasing the likelihood of unwise or even illegal government action. Finally, classification is expensive—and overclassification wastes taxpayer money.

1. Risks to National Security

Needless secrets undermine national security in at least two ways. First, overclassification atomizes intelligence, blocking the exchange of information among and within government agencies. This makes it more difficult to draw connections between discrete pieces of information, including connections that may be necessary to stop terrorist attacks and other threats. Second, overclassification erodes government employees' respect for the classification system and increases the number of people who require access to classified information in order to do their jobs—two developments that greatly increase the risk of leaks.

Excessive secrecy undermines intelligence efforts by inhibiting information sharing. There are legitimate reasons why information is not shared in some cases, including not only national security concerns, but also privacy considerations that make the sharing of certain types of information inappropriate (e.g., personal information about individuals for whom there is no objective basis to suspect wrongdoing).[42] But needless or overly rigid restrictions on information sharing can jeopardize national security. The 9/11 Commission, for example, catalogued failures by federal agencies to share information with each other in the months leading up to the September 11 attacks, including the CIA's failure to inform the FBI that one of the future hijackers had entered the United States and that another had obtained a U.S. visa.[43] According to the Commission:

> What all these stories have in common is a system that requires a demonstrated 'need to know' before sharing …. Such a system implicitly assumes that the risk of inadvertent disclosure outweighs the benefits of wider sharing. Those Cold War assumptions are no longer appropriate.[44]

Despite efforts to encourage broader information sharing after 9/11, the problem has persisted. At the end of 2008, the Homeland Security Advisory Council, responding to a request from then-Secretary Michael Chertoff, issued a report entitled *The Top Ten Challenges Facing the Next Secretary of Homeland Security*. The Committee reported that "[t]he federal security clearance process and classification system is broken and is a barrier (and often an excuse) for not sharing pertinent information with homeland security partners."[45]

Similarly, a 2010 report by the top U.S. intelligence official in Afghanistan, which recommended sweeping changes in intelligence gathering as a part of counterinsurgency strategy, underscored the importance of limiting classification to promote information sharing. The report stressed the need for ground-level intelligence about conditions in Afghanistan and warned that "[s]ome reports … [are] 'stove-piped' in one of the many classified-and-disjointed networks that inevitably populate a 44-nation coalition."[46] The report called for the creation of information centers to collect intelligence on key districts in Afghanistan, with each center staffed with "a Foreign Disclosure officer whose mission will be to ensure the widest possible dissemination by pushing for the lowest classification."[47]

The problem is particularly acute with respect to information sharing among federal, state, and local officials. Whereas national security was once a predominantly federal matter, state and local law enforcement agencies increasingly are at the forefront of domestic counterterrorism efforts. As Secretary of Homeland Security Janet Napolitano has stated, "Homeland security begins with hometown security."[48] Tools such as fusion centers[49] and Joint Terrorism Task Forces[50] are designed to promote cooperation and information sharing among local law enforcement and federal agencies. Yet, state and local officials are frequently unable to obtain key information in a timely manner (or at all, in some cases) because it is classified. As the Chief of Police for the District of Columbia Metropolitan Police Department stated in congressional testimony:

> Access to federal intelligence information remains a major obstacle for local law enforcement. While the security classification system that mandates security clearances helps to ensure that sensitive information is protected, it also hinders local homeland security efforts. Information collected by the federal government is sometimes overly classified, causing valuable information that should be shared to remain concealed.[51]

While better procedures for granting timely clearances to the right people would improve matters, there will always be cases in which the "need to know" arises before the relevant personnel can be identified and cleared. For that reason alone, it is critical that classification be limited to those cases in which it is strictly necessary.

Unnecessary secrecy also threatens national security by undermining respect for the classification system and thereby promoting leaking by government officials. Although leaks of *improperly* classified information generally pose little threat to national security, lack of respect for the classification system increases the risk of innocuous and dangerous leaks alike. As early as 1956, the Coolidge Committee found a "casual attitude toward classified information" within the Defense Department[52] and went so far as to liken the overclassification problem to prohibition in the 1920s—people will not follow rules they do not respect:

> Generally speaking, it is very difficult in this country to enforce compliance with rules if those rules are not widely accepted as both necessary and reasonable. The failure of prohibition in the 1920's is the classic example.
>
> …
>
> When much is classified that should not be classified at all, or is assigned an unduly high classification, respect for the system is diminished and the extra effort required to adhere faithfully to the security procedures seems unreasonable.[53]

As Supreme Court Justice Potter Stewart would later put it, "[W]hen everything is classified, then nothing is classified."[54]

The same problem persists today. Although lack of respect for the classification system is not the only cause of leaks, it remains a significant threat to information security. In the words of the former head of the government office that oversees classification: "The thing that protects information is not the markings, it's not the safes, it's not the alarms … it's people …. Once individuals start losing faith in the integrity of the process, we have an uphill road in terms of having people comply."[55] Accordingly, "[t]o allow information that will not cause damage to national security to remain in the classification system, or to enter the system in the first instance, places all classified information at needless increased risk." [56]

Overclassification erodes information security in another way as well. When so much information is needlessly classified, even those government employees and contractors who perform relatively low-level or non-sensitive jobs may require access to classified information to do their work. That is one reason why the pool of individuals who are authorized to have access to classified information has become so large—more than 2.4 million people, according to a 2009 report by the United States Government Accountability Office.[57] The larger the pool of people who have access to national security information, the greater the chance that the pool will include some people who handle the information irresponsibly. Bad apples are simply inevitable in a barrel that contains so many apples.

The recent WikiLeaks disclosures—involving the unauthorized release of more than 75,000 documents from a collection of U.S. military logs of the war in Afghanistan, nearly 400,000 U.S. Army field reports from Iraq, and more than 250,000 cables from U.S. embassies around the world[58]—show what can happen when those who have access to classified information do not respect the system and when the wrong people are granted clearances. These historic leaks demand a reevaluation of information security practices, but the need to protect information that is properly classified (e.g., by rigging classified computer systems to issue an alert if large numbers of documents are downloaded by a single user) should not be confused with the need to classify documents in the first place. Indeed, classified information is easier to protect when there is less of it. As Thomas Blanton, Director of the National Security Archive, testified before the House Judiciary Committee, "We have to recognize that right now, we have low fences around vast prairies of government secrets, when what we need are high fences around small graveyards of the real secrets."[59]

Unfortunately, the lesson that many observers appear to have drawn from the WikiLeaks disclosures is that we must crack down on those who publish leaked information.[60] Leaving aside the First Amendment implications of such an approach (which are beyond the scope of this report), the government employees who leak the information in the first place have always been subject to harsh legal sanctions—indeed, as discussed below, they must sign documents acknowledging criminal liability for unauthorized disclosures. The threat of legal sanctions is simply insufficient to deter leaks in a system in which those who are entrusted with classified information have so little faith in the integrity of classification designations. As long as overclassification remains rampant, there will be those who see no harm in leaking classified information and/or who believe they are performing a public service by doing so—and the nation will continue to face the risk that such leaks will include secrets genuinely worth keeping.

2. Harm to Democratic Decision Making

Information is the critical ingredient to responsible self-governance. James Madison famously wrote that "[a] popular Government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or perhaps both. Knowledge will forever govern ignorance; And a people who mean to be their own Governors must arm themselves with the power which knowledge gives."[61] The people require knowledge of their government's actions and intentions in order to debate the issues of the day and help shape the policies developed by their elected representatives. They require such knowledge in order to hold their representatives accountable at the ballot box for choices that do not reflect their wishes. And they require such knowledge in order to seek redress in the courts for actions that contravene the law.

Withholding information allows the executive branch to insulate itself from public criticism and, in some cases, congressional and judicial oversight, which in turn increases the likelihood of unwise, illegal, and improper activity. Consider, for example, the 1947 Atomic Energy Commission memo that ordered information about radiation experiments on humans to be classified because disclosure "might have [an] adverse effect on public opinion."[62] The memo clearly sought to head off public opposition to the government's experiments. At the same time, the memo sought to place a thumb on the other side of the public opinion scale by permitting disclosure of favorable information about the effects of nuclear radiation on humans—specifically, "documents regarding clinical or therapeutic uses of radioisotopes and similar materials beneficial to human disorders and diseases."[63]

More recently, the executive branch used the classification system to conceal legal defenses of torture prepared by Department of Justice lawyers within the Office of Legal Counsel (OLC). Not only were the actual interrogation techniques classified (the propriety of which can be debated);[64] so, too, was the legal analysis claiming that the statutes prohibiting torture do not apply to the President acting as Commander in Chief, and that the infliction of pain amounts to torture only if the pain approximates the sensation of "death, organ failure, or serious impairment of body functions."[65] In the absence of a presidential override, this legal analysis was binding on the executive branch and therefore constituted a type of "secret law," the classification of which was wholly inappropriate, according to congressional testimony of the former government official chiefly responsible for overseeing classification. This former official noted that learning about the memos years later was akin to "waking up one morning and learning that after all these years, there is a 'secret' Article to the Constitution that the American people do not even know about."[66]

The torture memos are a prime example of how secrecy can lead to unsound reasoning by policymakers and undermine democratic decision making. The improper classification and highly restricted distribution of certain OLC lawyers' interpretation of the torture statutes prevented other government lawyers, including other lawyers within the Justice Department, from testing the legal soundness of the opinions. Had this occurred, the memos might never have been issued; instead, they remained in place for several months until a new head of OLC concluded that their legal reasoning was flawed and withdrew them.[67] Equally troubling, the secrecy of the program itself prevented the public and Congress from debating, before the fact, the question of whether the United States should torture detainees in an effort to acquire intelligence. Whether one supports or opposes the use of torture, the decision to use it redefined our national identity and—through its effect on how others perceive us—may change the course of our history. The hallmark of a democracy is that the people have both a right and an obligation to participate in such consequential decisions.

3. Financial Costs

According to the government office that oversees classification, the government spent $10.17 billion on security classification in fiscal year 2010, the most recent year for which figures are available. This estimate includes such functions as clearing government employees for access to classified information, physically safeguarding facilities that hold classified information, and blocking unauthorized access.[68]

The public estimate, however, does not include the classification budgets of some of the largest intelligence agencies—including the CIA, the Defense Intelligence Agency, the National Security Agency, and the Office of the Director of National Intelligence—because the amount of money these agencies spend on classification is *itself* classified.[69] The real annual cost of classification, then, significantly exceeds $10.17 billion.

Experts studying classification have repeatedly noted that the government would save money by reducing overclassification. In 1994, the Joint Security Commission reported that "[o]verhauling the classification system will have cost-beneficial impacts on virtually every aspect of security …. [I]f we classify less and declassify more, we will have to clear fewer people, buy fewer safes, and mount fewer guard posts."[70] Similarly, the Moynihan Commission reported that "[t]he importance of the initial decision to classify cannot be overstated. Classification means that resources will be spent throughout the information's life cycle to protect, distribute, and limit access to information that would be unnecessary if the information were not classified."[71]

Of course, one would not necessarily expect any reduction in the amount of classified information to be accompanied by a proportionate reduction in costs, as some of the costs of classification—such as the cost of maintaining classified computer systems—are less sensitive to volume. Nonetheless, while there appear to be no studies of how much money the government would save by reducing overclassification, some classification costs, by their nature, depend on the volume of classified records and would shrink as overclassification declined. To give just one example, paper printouts of classified information must be stored in safes or special filing cabinets; a 1993 General Accounting Office study found that the average cost to the government of a regular five-drawer legal size filing cabinet with a single lock for unclassified information was $174.17, while the average cost of the equivalent container for classified information was $2,160.[72]

In any event, if overclassification indeed occurs at a rate of 50 percent or more (as government officials estimate), there is simply no question that curbing overclassification would significantly cut costs. At a time when federal spending on programs from Medicare to national defense may face deep cuts and the nation faces potential default on its debts, the United States can ill afford to continue spending enormous sums to protect information that does not require protection.

• • •

When the classification system prevents disclosures of information that could damage national security, it protects our safety and thus may justify the costs—to transparency and to the Treasury—that it incurs. Needless secrecy, however, causes real and substantial harm without any countervailing benefit. The problem of overclassification is accordingly a serious one, meriting careful analysis in order to arrive at a workable solution.

II. HOW CLASSIFICATION WORKS

The rules that define the modern classification regime reside primarily in an executive order issued by the President. Chief executives since Franklin Roosevelt have promulgated such orders,[73] and President Obama issued the current incarnation, Executive Order 13,526, in December 2009.[74] This chapter summarizes how classification operates under the current order, including what standards govern classification, how access to classified information is controlled, how documents become declassified, and what oversight mechanisms exist.

Classification begins with original classifiers (also known as "original classification authorities" or "OCAs"), who are the only officials empowered to determine what information merits classification in the first instance. These officials both classify information themselves and prepare classification guides that define categories of information that require classification. Derivative classifiers, in turn, classify records that either incorporate information from previously classified documents or fall into categories specified in classification guides. In theory, every classification action by a derivative classifier must be traceable to a decision by an original classifier.[75]

Various mechanisms exist to declassify records, but the fact remains that a document, once classified, will likely remain classified—and unreviewed with respect to whether it should be classified—for many years.

A. Original Classification

Original classifiers tend to be high-level officials and must be designated in writing by the President, the Vice President, selected agency heads, or senior agency officials with "Top Secret" original classification authority.[76] At one time, there were more than 13,000 original classifiers.[77] In recent decades, however, successive administrations have made a concerted effort to reduce that number. In fiscal year 2010, the number of original classifiers reached an all-time low of 2,378 (although the number of original classification *decisions* increased from the previous year).[78]

1. Standard for Original Classification

Under the executive order, an original classifier may classify information only after determining that "the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security."[79] The level of classification—Confidential, Secret, or Top Secret—depends on the level of possible damage to national security. Information may be classified as "Confidential" if its disclosure reasonably could be expected to "cause damage to the national security"; as "Secret" if its disclosure reasonably could be expected to "cause *serious* damage to the national security"; and as "Top Secret" if its disclosure reasonably could be expected to "cause *exceptionally grave* damage to the national security."[80]

In addition to its disclosure posing a risk to national security, information must fall into specified categories in order to be classified. Such categories include, for example, "military plans, weapons

systems, or operations," and "intelligence activities (including covert action), intelligence sources or methods, or cryptology." Section 1.4 of the executive order lists these categories.[81]

The language of the executive order contains several restrictions aimed at limiting overclassification. For example:

> To classify a document, an original classifier must be "able to identify or describe the damage" to national security that disclosure could cause.[82]
>
> Officials must not classify documents to "conceal violations of law, inefficiency, or administrative error," or to "prevent embarrassment to a person, organization, or agency."[83]
>
> "Basic scientific research information not clearly related to the national security shall not be classified." [84]

These provisions existed under previous executive orders and remain in force under the current order. In addition, President Obama's executive order contains a requirement, similar to one included in President Carter's executive order but removed by President Reagan,[85] designed to further limit unnecessary classification: "If there is significant doubt about the need to classify information, it shall not be classified."[86]

2. Duration of Original Classification

In addition to assigning the appropriate classification level, the original classifier must determine the date or event that will trigger declassification, "based on the duration of the national security sensitivity of the information."[87] The original classifier must assign a date or event that is ten years in the future or less, unless the original classifier "determines that the sensitivity of the information requires" that it remain classified for a longer period, up to twenty-five years.[88] An original classifier may classify a document for more than twenty-five years only if information that it contains "should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction."[89] Moreover, President Obama's executive order provides for the first time that "[n]o information may remain classified indefinitely."[90]

In theory, when the date or event specified by the classifier arrives, the information becomes "automatically declassified"—but "automatic" declassification tends to be a slow and laborious process.

Classifiers often mark documents for long periods of secrecy. While the proportion of documents marked for classification for ten years or less reached an all-time high of 74 percent in fiscal year 2010, this figure still means that original classifiers classify documents for more than ten years a quarter of the time.[91]

In theory, when the specified event occurs or the specified date arrives, the information becomes "automatically declassified."[92] As discussed below, however, "automatic" declassification tends to be a slow and laborious process that delays release even after the triggering event or marked date.

3. Original Classification Markings and Document Preparation

Original classifiers must annotate classified documents with certain markings. First, the document must show the overall classification level (Confidential, Secret, or Top Secret), which reflects the highest level of classification for any information in the document.[93] This marking appears in capital letters at the top and bottom of each page, except that some internal pages may instead display the highest classification level for the information on that page. Original classifiers must also "portion mark" classified documents, meaning that they must indicate the classification level of each paragraph or other discrete segment (e.g., bullet point or graphic display).[94] Classifiers generally mark paragraphs with a "U," "C," "S," or "TS," meaning "Unclassified," "Confidential," "Secret," or "Top Secret."

Second, the document must include the identity of the classifier, either by name and position or by personal identifier.[95] Third, the document must list the agency or office in which the document originated, if not otherwise evident.[96] Fourth, the document must contain declassification instructions, including the date or event that will trigger declassification or special markings for documents classified for more than 25 years.[97]

Fifth, an original classifier must note on the document "a concise reason for classification that, at minimum, cites the applicable classification categories."[98] As noted above, Section 1.4 of the executive order lists the classification categories, such as "military plans, weapons systems, or operations."[99] In practice, original classifiers comply with the "concise reason" requirement by referring to the subsections of Section 1.4 rather than by providing a narrative reason. For example, an original classifier would list "1.4(a)" as the reason for classifying information that involves military plans, weapons systems, or operations because this category appears in Section 1.4(a) of the executive order.

Finally, in cases where "classified information constitutes a small portion of an otherwise unclassified document," the executive order requires classifiers to use a classified addendum "whenever practicable."[100] Segregating all classified information to such an addendum allows the rest of the document to remain unclassified and thereby helps to limit overclassification. Alternatively, if practicable, classifiers may "prepare a product to allow for dissemination at the lowest level of classification possible or in unclassified form."[101]

B. Derivative Classification

Individuals who require access to classified information in the course of their work often have the need to reiterate this information, whether in communications with their colleagues or simply in their own work. Each document or communication that contains the information must itself be properly classified. Accordingly, the universe of derivative classifiers is in theory coextensive with the universe of individuals who are authorized to have access to classified information—a pool that includes more than 2.4 million people.[102]

Derivative classification can occur in two ways. First, derivative classifiers classify new documents that incorporate information already classified by an original classifier in another document. The

executive order requires derivative classifiers to "carry forward to any newly created documents the pertinent classification markings," and provide "a listing of the [classified] source materials."[103] Like original classifiers, derivative classifiers must also "portion mark" each paragraph with its classification status.[104]

Second, derivative classifiers classify information based on standards and categories contained in agency classification guides. Such guides, numbering approximately 2,500 throughout the federal government,[105] are prepared by original classifiers.[106] Because derivative classifiers lack authority to determine on their own whether the release of information would harm national security, application of the guides is intended to be a fairly mechanistic exercise, akin to classifying information that originated from a classified source document. In practice, however, broad criteria contained in some classification guides often require derivative classifiers to exercise a high level of discretion. Consider, for example, the following excerpt from State Department criteria for classifying information on United States involvement in international disputes:

> In those cases where the U.S. has been, or may again be, involved as an intermediary, it is an additional concern that information not be released which would prejudice future negotiations on unresolved issues or impair the U.S.'s ability to continue an intermediary role to resolve those issues. For this reason, it is important that information be classified when its release might cause or revive conflict or controversy, inflame emotions, or otherwise prejudice U.S. interests.[107]

As this example suggests, derivative classifiers, like original classifiers, often must make difficult judgment calls.

The volume of derivative classification dwarfs that of original classification by a factor of 340 to 1. Derivative classifiers made 76,571,211 decisions to classify documents in fiscal year 2010, while 224,734 original classification decisions occurred in the same period. These figures actually understate the case because some agencies are not yet capturing all classified electronic documents in their count.[108]

President Obama's executive order imposes several new requirements on derivative classifiers. Rather than remaining anonymous, as had previously been the case, derivative classifiers must now identify themselves on the documents they classify.[109] When practicable, they must also use classified addendums if only a small portion of a document contains classified information, or prepare a product that can be disseminated at the lowest possible classification level or in unclassified form.[110] The new order also adds a training requirement for derivative classifiers, who must receive training "in the proper application of the derivative classification principles of the [executive] order, with an emphasis on avoiding over-classification, at least once every 2 years."[111]

C. Access to Classified Information

The executive order on classification specifies that "[a] person may have access to classified information provided that: (1) a favorable determination of eligibility for access has been made by an agency head or the agency head's designee; (2) the person has signed an approved nondisclosure agreement; and (3) the person has a need-to-know the information."[112]

The first requirement—the determination of eligibility for access—entails a process commonly known as granting or obtaining a "clearance," which is governed by an executive order on access to classified information and implementing regulations.[113] Applicants for a security clearance must complete a form in which they provide information regarding residence, education, and employment history; family and associates; foreign connections and travel; arrests; illegal drug use; financial delinquencies; mental health counseling or counseling for substance abuse; and other personal information. The number of years for which applicants must provide historical information depends on the level of clearance sought. For example, applicants must provide residence, education, and employment information going back ten years in order to obtain a Top Secret Clearance, while only seven years' worth of such information is required for a Secret clearance.[114]

An extensive background check is then conducted to determine whether the applicant's "personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information."[115] For applicants seeking Confidential or Secret clearances, the investigation consists of a credit bureau report and a review of records held by federal agencies and local criminal justice agencies. For applicants seeking a Top Secret clearance, the investigation additionally includes a limited investigation into the applicant's spouse; interviews of the applicant, any former spouse(s), and references; and reviews of rental, employment, and academic records. Applicants who are granted clearances are subject to periodic reinvestigations; how often the reinvestigations occur and what they entail depend on the clearance level.[116]

In addition to obtaining a clearance, individuals seeking access to classified information must sign a nondisclosure agreement. The agreement references applicable restrictions on handling and disclosure of classified information, and the signatory acknowledges that a violation of these restrictions may result in the termination of his or her clearance, removal from any position of "special confidence and trust" requiring such a clearance, or termination of employment.[117] The form further states, "I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws"—followed by a list of specific statutory provisions.[118]

Finally, cleared individuals who sign a nondisclosure form may gain access to classified information at the level of their clearance only if they have a "need to know" the information in order to perform their duties. The "need to know" determination, which must be undertaken by anyone with authorized access to classified information prior to sharing it, is often fairly *ad hoc* in nature. Additional restrictions on access may be formalized, however, through the designation of Sensitive Compartmented Information ("SCI") or Special Access Programs ("SAP"). These designations create particular "compartments" or programs to which only a specified subset of individuals, as approved by a government program office or other entity, have access. Such programs, which are usually but not always classified at the Top Secret level, may come with their own handling restrictions, and some are considered so sensitive that they are hidden among other entries in the U.S. budget.[119]

D. Declassification

Declassification occurs through two primary mechanisms. First, "automatic" declassification occurs when the date or event for declassification specified by the classifier arrives or, subject to certain exceptions, after twenty-five years. Second, when triggered by requests from the public or challenges raised by persons with authorized access to classified information, review may occur before the specified date or the twenty-five-year mark arrives. These mechanisms are described below in greater detail.

1. "Automatic" Declassification at Specified Dates

The executive order provides that, when the date or event established by the classifier arrives, "the information shall be automatically declassified."[120] Similarly, regardless of when a document has been marked for declassification, the executive order provides that it shall be "automatically declassified" twenty-five years from its origin.[121]

When documents reach twenty-five years of age, agencies may exempt them from declassification if they fall within nine categories, such as records that "should clearly and demonstrably be expected" to "reveal information, including foreign government information, that would cause serious harm to relations between the United States and a foreign government, or to ongoing diplomatic activities of the United States."[122]

Agencies may exempt categories of information after fifty or seventy-five years if they fall into more narrow categories. An agency may exempt information from declassification after fifty years only if release "should clearly and demonstrably be expected to reveal" either "the identity of a confidential human source or a human intelligence source," or "key design concepts of weapons of mass destruction."[123] Documents may remain classified for more than seventy-five years after their origin only if an agency head proposes an exemption and the Interagency Security Classification Appeals Panel (ISCAP), a body that consists of senior officials designated by the heads of several agencies, approves the proposal.[124]

In practice, "automatic" declassification is a misnomer. President Clinton's executive order introduced the concept of automatic declassification in 1995, directing that documents would be declassified at the twenty-five-year mark "whether or not the records have been reviewed."[125] The order gave agencies a five-year deadline to declassify documents twenty-five years or older, except documents that fell into certain specified categories.[126] The expectation was that agencies would declassify such documents without page-by-page review.[127]

However, agencies proved reluctant in many cases to declassify documents without closer scrutiny, and in 1998, Congress enacted a provision that requires page-by-page review of many documents subject to automatic declassification under the executive order. The provision, known as the Kyl-Lott Amendment and contained in 50 U.S.C. § 2672, requires page-by-page review of all documents for information about atomic weapons or nuclear material, unless the documents "have been determined to be highly unlikely to contain" such information.[128] Moreover, because the executive order establishes a general rule that only the agency that creates classified information can declassify it, an agency reviewing a document that includes classified information originating from other agencies must refer the document to those agencies to perform their own review prior to declassification.[129]

With page-by-page review and review by multiple agencies occurring in many cases, the five-year deadline in President Clinton's executive order for declassification of most documents more than twenty-five years old came and went. Subsequent executive orders have granted repeated extensions.[130] The records are held by the National Archives and Records Administration (NARA), which is charged with collecting from the agencies, and then preserving, records of historical value.[131] At present, sixteen years after President Clinton first announced the five-year deadline for "automatic" declassification of certain records, NARA faces a backlog of over 400 million pages of classified records more than twenty-five years old.[132]

President Obama's executive order established a National Declassification Center, designed to coordinate the referral of such documents to the relevant agencies for declassification review (among other responsibilities) and thereby to eliminate the backlog. It remains to be seen whether the National Declassification Center and the agencies will meet the new deadline—December 31, 2013—that the order sets for reviewing the records.[133]

2. Review Before the Marked Date

Declassification can occur before the marked date or event through three primary mechanisms: requests for declassification review by members of the public, Freedom of Information Act requests, or classification challenges by authorized holders of classified information.

Mandatory Declassification Review: Members of the public may submit requests for classified documents through a process known as "mandatory declassification review" (MDR). An individual must submit his or her request to the agency that originated the document, describing "the document or material containing the information with sufficient specificity to enable the agency to locate it with a reasonable amount of effort."[134] In response to such requests, agencies must declassify information that does not meet (or no longer meets) the standards for classification. If unsatisfied with the initial decision, the requester may file an administrative appeal within the agency. Following that appeal, the requester may appeal to ISCAP (described in more detail below). If ISCAP orders information declassified, only the President can override the decision.[135]

MDR has been remarkably effective at accomplishing the declassification of requested documents. Between fiscal years 1996 and 2010, agencies received 75,581 MDR requests. After initial review, only 8 percent of classified pages remained classified in their entirety. At the agency appeal level, agencies in fiscal year 2010 declassified 61 percent of the pages reviewed in whole or in part; and at the ISCAP appeal level, the panel declassified 68 percent of the pages reviewed in whole or in part. Nonetheless, the effectiveness of the MDR program as a tool for accomplishing declassification system-wide is limited by the relatively small number of requests processed—an average of 4,393 requests per year, contrasted with the nearly 77 million classification decisions made in fiscal year 2010.[136]

Freedom of Information Act Requests: Individuals may also make requests for agency records under the Freedom of Information Act (FOIA). If the agency refuses to release records, the requester may appeal the determination within the agency, and ultimately may bring a federal lawsuit to obtain the documents. The agency, however, need not release records that fall within certain statutory exemptions, including an exemption for records that are authorized to be classified under the executive order and are "in fact properly classified" under the order.[137] Some agencies have procedures for reviewing whether classified documents requested under FOIA meet the executive order's criteria for classification.[138] FOIA challenges have proven to be far less effective than MDR, however, in obtaining the declassification and release of classified

information. In FOIA cases, as one expert notes, courts have "adopted a deferential posture to the executive branch on national security matters," and they "almost never overturn agency classification decisions."[139]

Classification Challenges: Under the executive order, "authorized holders" of classified information (i.e., individuals who are authorized to have access to the information) are "encouraged and expected to challenge the classification of information that they believe is improperly classified or unclassified."[140] The order provides that those who challenge classification decisions must not be "subject to retribution" and have a right to appeal agency decisions to ISCAP.[141] Authorized holders brought 722 formal challenges in fiscal year 2010, 16 percent of which resulted in the classification status of the document being partially or entirely overturned.[142] The markedly lower success rate for internally-brought challenges than for MDR in part reflects differences between the two types of challenges—MDR requests are more likely to involve historical documents, for instance, and internally-brought challenges include challenges to the *unclassified* status of information—but it may also suggest the need for a process that allows authorized holders to bring challenges anonymously (discussed further below).

E. Classification Oversight

The primary body that oversees the classification system is a small office within NARA: the Information Security Oversight Office (ISOO), established by President Carter in 1978.[143] ISOO's duties include, among others, issuing directives to implement the provisions of the executive order, reviewing agencies' implementing regulations, conducting on-site reviews of agency classification programs, and recommending presidential action on requests for original classification authority.[144]

Based on information submitted by agencies, ISOO issues an annual report to the President that provides statistics ranging from the number of original classifiers, to the number of classification decisions made, to the number of pages declassified.[145] ISOO also reviews samples of selected agencies' classified product—examining approximately 2,000 documents each year in recent years—and summarizes the results in its annual reports.[146] ISOO's annual reports also describe the results of on-site reviews of agency program management, self-inspection programs, and security education and training programs, as well as information about agencies' classification guides and declassification efforts.[147]

The executive order states that if the Director of ISOO finds a violation of classification standards or procedures, "the Director shall make a report to the head of the agency or to the senior agency official [in charge of the agency's classification program] so that corrective steps, if appropriate, may be taken."[148] The order provides that government officials and others with access to classified information (such as cleared contractors) are subject to sanctions "if they knowingly, willfully, or negligently" commit certain violations, such as disclosing classified information to unauthorized persons or "classify[ing] or continu[ing] the classification of information in violation of this order or any implementing directive."[149] According to the order, "[s]anctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions…"[150] However, ISOO is not empowered to impose such sanctions itself.

The executive order also gives ISOO the power to "require … information to be declassified by the agency that originated the classification" if the ISOO Director "determines that [the] information is

classified in violation" of the executive order.[151] An agency may appeal such a declassification order to the President through the National Security Advisor.[152] In practice, the existence of the power to order declassification has obviated the need to use it, as ISOO generally accomplishes the declassification of documents through informal exchange with agencies rather than fiat.[153]

The executive order also establishes ISCAP, which, as noted above, consists of senior-level government officials appointed by certain agencies that engage in classification. Currently, the agencies represented on the panel include the Departments of State, Defense, and Justice, NARA, the Office of the Director of National Intelligence, the National Security Advisor, and (in some cases) the CIA. The panel rules on appeals regarding classification challenges brought by authorized holders, as well as requests for mandatory declassification review filed by members of the public, and it reviews agency requests for exemption from automatic declassification requirements.[154]

Congress has also established an executive advisory committee called the Public Interest Declassification Board. The Board's functions include, among others, advising the President and other executive branch officials on classification and declassification policy. The Board consists of nine members, five appointed by the President and four appointed by the ranking majority and minority members of the House and Senate.[155] The 2009 changes to the executive order on classification reflected recommendations by the Board; in developing these recommendations, the Board consulted stakeholders and solicited public input both online and at public meetings.[156] At the time of writing, the Board is developing recommendations for a "more fundamental transformation" of the classification system, as directed by the President, and recently completed a similar process of soliciting and receiving public input.[157]

Congress, too, plays an important role in classification oversight. As a threshold matter, Congress has supplemented the classification regime set forth in executive orders through statutes, such as the Atomic Energy Act, that require the protection of specified types of information. Congress also has enacted legislation to ensure that the rules governing access to classified information comport with certain due process standards. And it has attempted to address overclassification through laws such as the Freedom of Information Act, which allows judges (as discussed above) to determine whether documents have been properly classified, and the recently passed Reducing Over-Classification Act, which requires agencies' Inspectors General to assess agencies' implementation of classification policies. Finally, congressional committees hold hearings to examine various issues relating to classification that fall within their jurisdiction; the testimony yielded by such hearings is cited throughout this report.

• • •

In summary, the classification system reflects a well-established set of procedures in which the executive order sets forth the criteria for classifying documents, original classifiers determine which information meets those criteria and for how long it must be classified, and derivative classifiers carry forward original classifiers' determinations or rely on guidance prepared by original classifiers. The effect of a classification decision is far-reaching: even government employees who hold clearances are barred from access if they cannot demonstrate a "need to know," and—despite the existence of various oversight bodies and means of seeking a document's declassification—a classified document will likely stay classified until, and in many cases long after, the date or event specified by the classifier.

III. WHY OVERCLASSIFICATION OCCURS

The previous chapter described how the classification system works—or at least how it is designed to work. This chapter describes how, in practice, the system breaks down. In short, the incentive structure underlying the current system, in which a multitude of forces pushes in the direction of classification while no force pushes meaningfully in the other direction, virtually ensures that overclassification will occur.

A. Incentives to Overclassify

Several forces unrelated to national security considerations push strongly in the direction of classifying documents. At the top of the list is a culture of secrecy that pervades many of the agencies that engage in classification. In addition, government officials have an obvious interest in shielding evidence of governmental misconduct or incompetence; public scrutiny and congressional involvement can slow down or prevent officials' desired course of action; officials who fail to protect sensitive national security information face harsh sanctions and, in some cases, public condemnation; and other demands on classifiers' time and attention discourage giving careful thought to classification decisions.

1. A Culture of Secrecy in Government Agencies

In his Chairman's Foreword to the 1997 Moynihan Commission report, Senator Moynihan noted that, during the Cold War, "[a] culture of secrecy took hold within American Government."[158] This culture was premised on the notion that we knew who the adversary was; we knew that the adversary's spies were attempting to learn military secrets; and we knew exactly who, among trusted federal officials, needed to know the information that we were trying to keep out of enemy hands.[159]

Many commentators have observed that this culture of secrecy has become a seemingly permanent feature of the national security establishment, even though the Cold War conditions and assumptions that arguably supported such a culture no longer obtain.[160] The 9/11 Commission, for example, commented that the emphasis on "need to know" within the classification system "implicitly assumes that the risk of inadvertent disclosure outweighs the benefits of wider sharing. Those Cold War assumptions are no longer appropriate."[161] For one thing, deciding who has a "need to know" is a difficult and error-prone undertaking when the identity of the enemy is in flux and both the means and the targets of attack are unpredictable. Moreover, given the transnational nature of the modern terrorist threat and its focus on civilian targets, information routinely must be shared among federal, state, local, and foreign governments, as well as partners in the private sector and even members of the public.[162] Nonetheless, as one member of the 9/11 Commission stated, the "unconscionable culture of secrecy [that] has grown up in our Nation since the cold war" remains.[163]

While the modern culture of secrecy within government may have its proximate genesis in the Cold War and the U.S. government's response to the Soviet threat, its roots in fact go much deeper—to the very nature of bureaucracies and human interaction. Francis Bacon observed in 1597 that "knowledge itself is power,"[164] and this truism carries a natural corollary: denying knowledge to others increases one's own power relative to theirs. Accordingly, as one scholar has noted, "Persons who possess sensitive information will seek to preserve the secrecy of those data as a way of enhancing their standing . . . vis-à-vis other agency employees."[165] Official secrets—those that come with a stamp—are of particular value in this power game: "In any culture, a crucial

method by which insiders retain their status is by determining who may remain within and who is to be an outsider in varying degree. Whenever an exclusion is sanctioned by the state, it carries particular weight."[166]

Government officials thus use classification to confer additional importance on the information they are conveying—and, by extension, on themselves. As stated by one journalist in recounting a conversation with a retired intelligence official:

> [The retired official] . . . noticed that classification was used not to highlight the underlying sensitivity of a document, but to ensure that it did not get lost in the blizzard of paperwork that routinely competes for the eyes of government officials. If a document was not marked 'classified,' it would be moved to the bottom of the stack, eclipsed by more urgent business, meaning documents that carried a higher security classification. He observed that a security classification, by extension, also conferred importance upon the author of the document. If the paper was ignored, so too was its author. Conversely, if the materials were accorded a higher degree of protection, they would redound to their author's credit and enhance his or her authority and bureaucratic standing.[167]

A leading expert in government secrecy recounted a similar exchange highlighting the perceived connection between a document's classification level and its importance: "A general once told me he only reads things that were marked 'Top Secret.' If it was less than that, it wasn't worth his time."[168]

Just as individuals may seek to enhance their standing within an agency, agencies seek to enhance their own power within government. In his seminal 1946 essay on bureaucracy, Max Weber observed that "[e]very bureaucracy seeks to increase the superiority of the professionally informed by keeping their knowledge and intentions secret."[169] Particularly since 9/11, generating and dealing in official secrets is almost a prerequisite for agencies to be taken seriously. In the words of one intelligence contractor, "You can't be a big boy unless you're a three-letter agency and you have a big SCIF"—a facility used for housing and viewing classified documents.[170]

Information control can be a key weapon in turf wars between agencies. This is particularly so in the field of national security, in which a number of agencies share responsibilities and must compete with one another for funding, access to the President, and prestige.[171] A former national security official under President Reagan estimated that "protection of bureaucratic turf" accounts for as much as 90% of classification,[172] while Senator Moynihan's study of the issue led him to conclude that "[d]epartments and agencies hoard information, and the government becomes a kind of market. Secrets become organizational assets, never to be shared save in exchange for another organization's assets."[173] Agencies may deny access to other agencies by excessive compartmentation or simply invoking the "need to know" requirement.[174] Alternatively, they may restrict the dissemination of information by classifying it inappropriately or at too high a level. For example, former intelligence officers told *Washington Post* reporters that "[t]he CIA reclassified some of its most sensitive information at a higher level so that National Counterterrorism Center staff, part of the [Office of the Director of National Intelligence], would not be allowed to see it."[175]

Organizational cultures affect everyone within the organization, and they tend to be self-reinforcing.[176] Accordingly, individual classifiers need not possess a Cold War mindset, a desire to enhance their own

importance or the perceived importance of their work, or a sense of competition with other agencies in order to be influenced by this phenomenon. In an agency characterized by a culture of secrecy, classification simply becomes "how we do things"—a manifestation of the culture that in turn perpetuates it.

2. Concealment of Information that Reveals Governmental Misconduct or Incompetence

Executive officials who are involved in instances of governmental misconduct or incompetence have an obvious motive to withhold information about those actions. The executive order bans classification intended to "conceal violations of law, inefficiency, or administrative error," or to "prevent embarrassment to a person, organization, or agency."[177] There is no mechanism, however, for monitoring and enforcing compliance with this provision. And even if such a mechanism existed, the prohibition is framed in such a way that it would be exceedingly difficult to prove its violation. The focus of the prohibition is the intent of the classifier, and as long as the classifier could posit some national security implication to releasing the information—however tenuous, implausible, or secondary—he or she could maintain that hiding wrongdoing was not the intent.[178]

Since its inception, the classification system has been used for the improper purpose of concealing governmental misconduct. As noted above, the Atomic Energy Commission in 1947 produced a memorandum on "Medical Experiments on Humans" which encouraged classification of documents that could sour public opinion or prompt lawsuits.[179] In the same vein, the CIA during the Cold War concealed the use of hallucinogens on unwitting persons in a behavior-modification program code-named MKULTRA.[180] In the 1950s, the government, after receiving funds from Congress for heavy duty military cargo planes, classified pictures showing that the aircraft "were converted to plush passenger planes."[181] When a member of the House Appropriations Committee sent a letter asking about the conversion, he "found that even his letter of inquiry was stamped 'Secret.'"[182]

A more recent example is the classification of the warrantless wiretapping program conducted by the National Security Agency during the administration of George W. Bush. At the time the program was implemented, the Foreign Intelligence Surveillance Act (FISA) required the government to obtain a warrant in order to wiretap any domestic communications or international communications involving a U.S. person. The program involved the capture of such communications without warrants and accordingly violated FISA.[183] While Justice Department lawyers advanced creative arguments to justify the program's legality,[184] it is difficult to escape the conclusion that the program was classified at least in part because of its shaky legal footing. The alternative explanation—that the program would have lost its effectiveness if it were disclosed—appears to be off the mark in light of the fact that the administration pressed for the continuation of warrantless wiretapping after the program's existence was revealed, and indeed succeeded in persuading Congress to amend FISA (publicly, of course) to allow aspects of the program to continue.[185]

Some insiders have deemed the use of classification to hide evidence of fraud, waste, or abuse to be among the most frequent causes of overclassification. Erwin Griswold, who served as Solicitor General under President Nixon and argued before the Supreme Court that the New York Times should be enjoined from publishing some of the contents of the Pentagon Papers, published an op-ed in the *Washington Post* nearly thirty years later in which he admitted that publication of the papers carried little if any risk to national security. He wrote, "It quickly becomes apparent to any person who has considerable experience with

classified material that there is massive overclassification and that the principal concern of the classifiers is not with national security, but rather with governmental embarrassment of one sort or another."[186] Similarly, in describing the classified documents he reviewed while serving on the Select Committee on POW/MIA Affairs, Senator John Kerry stated that "more often than not they were documents that remained classified or were classified to hide negative political information, not secrets."[187]

3. Facilitation of Policy Implementation

From the early days of the Republic, it has been well understood that one of the primary advantages of secrecy is that it enables executive officials to act quickly and easily, unencumbered by the slow workings (and uncertain outcomes) of the democratic process. The Founders' writings are replete with references to the ability of the executive branch to act with "secrecy" and "dispatch"; indeed, the two terms routinely appear together.[188] The reason is obvious: public debate and the legislative process tend to slow almost any political initiative. Instances in which the executive branch, Congress, and the public coalesce quickly behind substantive new policy are more likely to occur under circumstances of national crisis (for example, the passage of the USA PATRIOT Act or the Authorization for Use of Military Force after 9/11[189]) and are notable for being the exception rather than the rule.

Indeed, even within the executive branch, the general rule holds true that the smaller the number of people involved in any initiative, the more quickly and smoothly it can be implemented. Alexander Hamilton had this fact in mind when he argued that there should be a single President heading the executive branch: "[D]ecision, activity, secrecy, and dispatch will generally characterise the proceedings of one man, in a much more eminent degree, than the proceedings of any greater number; and in proportion as the number is increased, these qualities will be diminished."[190] This principle has legitimate applications, to be sure—including, most notably, the choice of our presidential system. But it can also find expression in the improper classification of government programs. Particularly when executive officials know that their desired course of action may raise eyebrows among colleagues, highly compartmented classification can be an attractive option. In the words of one former CIA official: "One of the tried-and-true tactical moves is if you are running an operation and all of a sudden someone is a critic and tries to put roadblocks up to your operation, you classify it and put it in a channel that that person doesn't have access to . . . ."[191]

Thus, when the FBI wiretapped Dr. Martin Luther King, Jr.'s telephone, it sought to exclude even the Attorney General from knowing about its activities, lest his involvement ultimately scuttle the initiative. In an internal memo, an FBI official stated:

> The attached document is classified "Top Secret" to minimize the likelihood that this material will be read by someone who will leak it to King. However, it is possible despite its classification, the Attorney General himself may reprimand King on the basis of this material. If he does, it is not likely we will develop any more such information through the means employed. It is highly important that we do develop further information of this type in order that we may completely discredit King as the leader of the Negro people.

FBI Director Hoover then wrote on the memo, "No. A copy need *not* be given the A.G."[192]

Classification similarly can be used to ease policy implementation by limiting or manipulating congressional involvement. For example, in the late 1980s, President Reagan sought to win congressional support for military aid to the government of El Salvador, which was fighting left-wing rebels. Some members of Congress, however, were concerned about the Salvadoran government's potential connections with right-wing paramilitary groups known as "death squads." In response to a FOIA request, the government released portions of a CIA report stating that Salvadoran military officers had pledged to punish human rights offenders—but classified and refused to disclose portions of the report concluding that the Salvadoran government was "incapable of undertaking a real crackdown on the death squads."[193] Through this selective classification, the administration was able to strengthen its case before Congress.

A similar, more recent example involves the efforts of the administration of George W. Bush to persuade Congress to authorize military force against the regime of Saddam Hussein in Iraq. The stated justification for military intervention—i.e., the hypothesis that Hussein had reconstituted various programs relating to weapons of mass destruction (WMDs)—was addressed at length in a classified National Intelligence Estimate (NIE). Only a handful of members of Congress saw the classified version of this NIE, in which the conclusions regarding Hussein's posited WMD programs were tempered by qualifying statements and dissent among agencies.[194] The remainder of Congress, as well as the public, was presented with an unclassified white paper that left out key information, including the identities of dissenting agencies and, on one key point, the entire dissenting opinion. A congressional investigative committee later found that the unclassified version left readers "with an incomplete picture of the nature and extent of the debate within the Intelligence Community regarding these issues."[195] Acting on incomplete information, Congress provided the President with the authority he sought.[196]

Secrecy enables executive officials to act quickly and easily, unencumbered by the slow workings and uncertain outcomes of the democratic process.

Finally, classification can be a tool to shape public opinion in support of controversial policies. After 9/11, the detention of persons that the executive branch deemed "enemy combatants" at Guantánamo Bay, Cuba, without charge and under conditions that many believed to be inhumane, became the subject of fierce public debate. In the face of this debate, members of the George W. Bush administration repeatedly made statements to the effect that the persons imprisoned at Guantánamo were "the worst of the worst" and that their indefinite detention was critical to national security.[197] The administration classified its actual assessments of the risks posed by specific detainees, however, including many cases in which the government could find no recorded reason for the detainee's transfer to Guantánamo.[198] By definition, the absence of any recorded reason for the detention of a given individual does not reveal any intelligence sources or methods, as there are no sources or methods to reveal. It is certainly possible that these documents were classified by rote, or based on an unduly expansive understanding of the categories of classifiable information under the executive order. But it is also undeniably true that disclosing the documents would have weakened the administration's public case for the necessity of its actions at Guantánamo.

In short, it is simply easier to get things done—particularly controversial things—when the involvement of other officials, Congress, and the public can be limited or controlled. It is thus tempting for executive

officials to act in secret or to be selective in their disclosure of information, regardless of whether the policy they seek to advance skirts the edges of the law or is squarely within the permissible bounds of government action.

4. Fear of Repercussions for Failing to Protect Sensitive Information

Classifiers who fail to protect sensitive national security information face serious repercussions, and the specter of such consequences—combined with the lack of consequences for improperly classifying documents (discussed further below)—provides a strong incentive to classify. This phenomenon has been noted by experts for half a century. The Coolidge Committee found that "[a] subordinate may well be severely criticized by his seniors for permitting sensitive information to be released, whereas he is rarely criticized for over-protecting it. There is therefore an understandable tendency to 'play safe' and to classify information which should not be classified, or to assign too high a category to it."[199] The Moss Subcommittee similarly found that "the Defense Department's security classification system is still geared to a policy under which an official faces stern punishment for failure to use a secrecy stamp but faces no such punishment for abusing the privilege of secrecy, even to hide controversy, error, or dishonesty."[200] And the 9/11 Commission observed that there are "risks (criminal, civil, and internal administrative sanctions) but few rewards for sharing information."[201]

Official sanctions aside, there is a natural tendency among government officials to be risk-averse when it comes to classification decisions. In the words of a former head of ISOO, "There is no underestimating the bureaucratic impulse to 'play it safe' and withhold information."[202] After all, in matters of national security, the perceived stakes are generally high, and perceived failures on the part of institutions or individuals entrusted with protecting national security are not looked upon kindly by the public—as evidenced, for example, by the widespread condemnation of the government's failure to anticipate and prevent the shooting deaths of thirteen people in November 2009 at the Fort Hood military post.[203]

No government official wants to be responsible for releasing information that leads to the next terrorist attack, regardless of how remote that possibility might be in a given instance. By contrast, the harms caused by overclassification, while grave and certain, are more dispersed and unlikely to be traced to any one government official. It is not surprising, under these circumstances, that government officials feel pressure to err—and to err liberally—on the side of classification.

5. Other Demands on Classifiers' Time and Attention

The threshold decision as to whether particular information meets the criteria for classification can be a difficult and time-consuming one (although the actual process of classifying documents is relatively easy, as discussed below). Original classifiers must engage in an inherently subjective judgment as to whether the disclosure of information "could reasonably be expected" to harm national security[204]—a judgment that may require them, in some instances, to consider a range of hypothetical scenarios and to assess the likelihood of each scenario unfolding. They also must determine whether the harm they foresee is best characterized as "damage," "serious damage," or "exceptionally grave damage,"[205] and they must attempt to predict the date on which the information will lose its sensitivity. Derivative

classifiers, if using a classification guide that contains vague standards, may be required to undertake a similarly subjective and complex analysis.

Although this analysis is required by the executive order and is essential to the integrity of the classification system, government officials who are occupied (and perhaps even overwhelmed) with other business—particularly those who deal with sensitive national security information on a daily basis—may feel that they do not have the luxury of engaging in it. The default position for these officials is classification, as they are far more likely to face adverse consequences if they fail to classify sensitive information than if they classify information that could safely be disclosed.[206] The press of business, when combined with the lack of accountability for improper classification decisions, thus leads directly to overclassification. This phenomenon was noted by the Project on National Security Reform, an independent organization that contracted with the Department of Defense, under instruction by Congress, to study the national security interagency system:

> [T]o decide not to classify a document entails a time-consuming review to evaluate if that document contains sensitive information. Former officials within the Office of the Secretary of Defense, for example, who often work under enormous pressure and tight time constraints, admit to erring on the side of caution by classifying virtually all of their pre-decisional products.[207]

The practice of saving time and effort by defaulting to classification interacts with, and reinforces, the culture of secrecy that exists in some agencies (as discussed above). Classifiers feel safe to follow this practice because they work in a culture in which secrecy is expected, not challenged. New employees, or those newly authorized to classify documents, quickly learn that classification by default is an acceptable time-saving option, and the practice becomes even more widespread. The result is a cycle in which a culture of secrecy fosters overclassification, which in turn fosters its own culture of secrecy, based more on habit than design.

B. Lack of Incentives to Refrain from or Challenge Overclassification

As the previous discussion demonstrates, there are several factors pushing officials to classify documents regardless of whether classification is warranted by national security considerations. There are few if any forces pushing in the other direction. Classification is a relatively (and increasingly) easy exercise; those who overclassify are not held accountable for doing so; classifiers receive inadequate training in the limits of their classification authority; and there are no rewards for those who challenge improper classification decisions.

1. Ease of Classifying Documents

As discussed above, classifiers make the sorts of difficult judgments that call for careful deliberation; yet the press of business often tempts classifiers to forego this exercise. The procedures for classifying information provide little safeguard against this temptation. To the contrary, several features of the current system allow government officials to classify documents without spending any time or effort considering whether classification actually is justified.

First, the executive order requires an original classifier to be "*able to* identify and describe the damage" to national security that could result from unauthorized disclosure[208]—but, under the current implementing directive, the classifier need not actually provide such an identification or description, in writing or otherwise, at the time of classification.[209] Because the system does not mandate an explanation, an original classifier can, in practice, classify a document even when he or she would not be able to identify any national security harm that might result from release.

Second, although the executive order states that only certain categories of information are subject to classification, classifiers need not explain why information falls into one of those specified categories. In 1995, President Clinton added to the executive order the requirement that original classifiers provide "a concise reason for classification which, at a minimum, cites the applicable classification categories in section 1.5 of this order [which now appear in section 1.4 of the current order]."[210] Two years later, the Moynihan Commission observed that the new requirement "can be satisfied by citing a relevant category of classifiable information." The Committee concluded that "[t]he current practice of merely citing one of the categories of classifiable information … does little to lessen the tendency to classify by rote and does not adequately reflect the long-term consequences of an original classification decision."[211] For example, merely writing the notation "1.4(b)" does not force the classifier to analyze whether information actually constitutes "foreign government information," an analysis under which a classifier may be required to assess whether the information was provided "with the expectation that the information, the source of the information, or both, are to be held in confidence."[212]

Derivative classification based on instructions in a classification guide requires even less explanation. The current implementing directive allows a derivative classifier to cite an entire classification guide, which may be tens or hundreds of pages, rather than the relevant paragraph of the guide that allows the information in question to be classified.[213]

Advances in technology have exacerbated the problem by automating much of the classification process. Classified documents generally are produced on classified computer systems. Many of these systems are designed not only to protect classified information, but to facilitate its classification. When creating a document or e-mail on these systems, classifiers are presented with drop-down prompts that can include default settings for the classification level or other required information.[214] Classification can be accomplished in this manner with a few quick (and unthinking) clicks of a mouse.[215]

Moreover, in the absence of any regular system for monitoring and enforcing compliance with the rules, even the few basic steps that classifiers are expected to take are too often dispensed with. For example, every classified document should contain a line that states "Classified By" (for original and, under the current executive order, derivative classifications) or "Derived From" (for derivative classifications), to ensure that the decision can be traced back to an original classification authority.[216] If the information in a derivatively classified document comes from more than one source document, the classifier may enter the phrase "multiple sources" on the "Derived From" line, but must maintain (or, under the current order, attach) a list of these sources.[217] In a typical year in which it conducted a document review at selected agencies, ISOO discovered that 18 percent of documents contained no "Classified By" or "Derived From" line, while 14 percent referenced "multiple sources" but no list of the sources could be found.[218] In another year, ISOO found that nearly a third of the documents reviewed were not properly portion marked.[219] In

its fiscal year 2009 report, describing the results of its document review at 15 agencies, ISOO observed that "[t]hree-fourths of the agencies had discrepancies in more than 50 percent of their documents; several agencies had error rates higher than 90 percent."[220]

In short, despite the consequential nature of the decision to withhold government information from the public, classifying documents in accordance with current rules is a fairly easy exercise—and classifying documents without regard to the rules is an even easier one. The first Justice Department memorandum authorizing waterboarding and other so-called "enhanced interrogation techniques" was simply stamped "Top Secret"; none of the other procedures for classification were followed.[221] By the simple act of placing those words on the top and bottom of every page, an unnamed government official withheld the details of the government's interrogation program from Congress and the public for years.

2. Lack of Accountability for Improper Classification

As noted above, government officials risk censure and other adverse consequences if they fail to classify documents that should be classified, but they have very little to lose when they classify documents unnecessarily. As the 9/11 Commission observed, "No one has to pay the long-term costs of over-classifying information, though these costs—even in literal financial terms—are substantial. There are no punishments for *not* sharing information."[222] The same observation about the lack of consequences for improper classification was made by the Coolidge and Moss Committees.[223] A former FBI official put it bluntly: "[I]t is a truism that no one ever got in trouble for over-classifying."[224]

This criticism is particularly noteworthy given that, on paper, the sanctions for overclassification have grown stronger over time. President Nixon's executive order provided that "[r]epeated abuse of the classification process shall be grounds for an administrative reprimand."[225] President Carter's executive order expanded the possible sanctions beyond administrative reprimand to include "reprimand, suspension without pay, removal, termination of classification authority, or other sanction in accordance with applicable law and agency regulations," and provided that officials would be subject to these sanctions if they "knowingly and willfully classif[ied] or continue[d] the classification of information in violation of this Order or any implementing directives."[226] Today's executive order contains similar provisions, and it strengthens sanctions by providing that negligent overclassification—in addition to knowing and willful overclassification—can subject the classifier to punishment.[227]

Even if agencies had an appetite for imposing such sanctions, however, there is no regular mechanism in place by which they could detect overclassification on the part of employees. The Stilwell Commission, studying the Department of Defense, reported in 1985 that "[c]urrent policy specifies that the signer of a classified document is responsible for the classification assigned but frequently, out of ignorance or expedience, little scrutiny is given such determinations."[228] In 1994, the Joint Security Commission proposed that each agency appoint an overclassification ombudsman who would "routinely review a representative sample of the agency's classified material" to enable "real-time identification of the individuals responsible for classification errors," with an eye toward "add[ing] management oversight of classification decisions and attach[ing] penalties to what too often can be characterized as classification by rote."[229] This recommendation, however, was not implemented.

The executive order governing classification does obligate each agency that has classification authority to maintain a self-inspection program, which must include a review and assessment of the agency's classified product.[230] But there is no requirement that the agency use this process to identify employees who are improperly classifying information, let alone hold them accountable. Moreover, in its annual reports, ISOO has consistently noted the failure of many agencies to maintain an adequate self-inspection program. In fiscal year 2005, for example, ISOO conducted on-site reviews at eighteen agencies and found that seven of them had no self-inspection programs whatsoever, while seven others had programs that did not include any review of classified documents.[231] Similarly, agencies frequently have failed in their obligation to include "management of classified information" as a critical element in the personnel performance ratings of those who regularly deal with classified information.[232] ISOO conducts its own review of agencies' classified product (as noted above), but can only undertake this review at a limited number of agencies each year.

Even strongly worded threats of punishment, such as those in the executive order, are ineffective unless there is a mechanism to measure compliance and a commitment to enforcing the rules. Remarkably, despite the increasing severity of the sanctions described in successive executive orders, it does not appear that a classifier has ever lost his or her classification authority or been terminated for overclassification.[233]

3. Inadequate Training on Proper Classification

Many of the factors that encourage overclassification could be countered by a strong training program that instilled in classifiers a proper understanding of, and respect for, the limitations of their authority. Successive executive orders on classification have long required that any person who is authorized to have access to classified information must "receive contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure."[234] Before the current iteration of the order, however, the only provision that addressed training in the proper classification of documents by original classifiers was a vague directive that "original classification authorities must receive training in original classification,"[235] and there was no requirement that derivative classifiers receive any training on making classification decisions. (President Obama's changes to the training provisions are discussed in Chapter 4 of this report.)

This regulatory gap was filled, to some degree, by ISOO's implementing directive, which included a general training requirement for "all executive branch employees who create, process, or handle classified information," and more specific training requirements for "personnel whose duties significantly involve the creation or handling of classified information."[236] Nonetheless, ISOO's annual reports routinely found that agencies failed to adhere to the training obligations specified in the executive order and implementing directive. For example, ISOO found that many agencies failed to provide any refresher training whatsoever, despite the requirement under the previous order and directive that such training be provided annually.[237] In its annual report for fiscal year 2008, ISOO reported that, "at one agency, a majority of the [original classifiers] did not receive training regarding their [classification] responsibilities."[238]

When training is provided, its content is often limited. Government officials report that their training has emphasized the need to protect classified information and that they have received little or no training on the limits of their classification authority—including the proper application of agency classification guides.[239] The results are predictable. According to the former head of ISOO, not only do classifiers frequently fail to adhere to the procedural requirements for classification (a failure that ISOO has attributed directly to insufficient training);[240] many derivative classifiers seem unaware that they lack authority to classify information that has not been deemed classified by an original classifier.[241]

4. No Rewards for Challenges to Improper Classification Decisions

The executive order on classification recognizes that individuals who are authorized to have access to classified documents are uniquely positioned to identify instances of overclassification. It accordingly provides that "[a]uthorized holders of information who, in good faith, believe that its classification status is improper are encouraged and expected to challenge the classification status of the information."[242] If the agency rejects the challenge, the authorized holder may appeal to ISCAP. The executive order directs agencies to establish procedures for bringing such challenges and prohibits retaliation against those who participate in the process.[243]

Yet classification challenges by authorized holders of classified information are rare. While there were nearly 77 million classification decisions made in fiscal year 2010, there were only 722 formal challenges brought by authorized holders and fewer than half that number the previous year.[244] Even if the level of overclassification among agencies were conservatively estimated to be ten percent (a much lower estimate than that employed by most experts),[245] that would still indicate that authorized holders brought formal challenges in only *one hundredth of one percent* of the cases in which such challenges would have been appropriate.

The reasons for the rarity of these challenges are evident. First, despite being directed to do so by the executive order, agencies do not in fact encourage classification challenges. Indeed, as the most recent ISOO report noted, "ISOO's program reviews have revealed that many authorized holders of classified information are not aware of this provision, and therefore, do not challenge classification decisions as much as should be expected in a robust system."[246] In some cases, ISOO found that agencies had put no procedures in place for authorized holders to bring such challenges.[247]

Second, there are no incentives to challenge improper classification decisions—and strong incentives not to challenge them. Neither the executive order nor the implementing ISOO directive provides any kind of reward or incentive to authorized holders who expend the time and effort to challenge a classification decision. On the other hand, the implementing ISOO directive states that authorized holders who wish to challenge classification decisions "shall present such challenges to an original classification authority [OCA] with jurisdiction over the information."[248] In some instances, this OCA may be the very person who made the decision that the authorized holder wishes to challenge. Even where that is not the case, an agency may have very few OCAs, and these individuals may not be sympathetic to subordinates who bring classification challenges. And even if a particular OCA is sympathetic, other agency officials who learn that an employee challenged a colleague's classification decision may not be. In short, particularly in an agency characterized by a culture of secrecy, there would be tremendous

peer pressure not to challenge the classification decisions of other employees. While the executive order prohibits retribution against challengers, such prohibitions can be extremely difficult to enforce—and they do not address the problem of employees being treated as "snitches" by their colleagues.

• • •

In summary, although the executive order that governs the classification system envisions a fairly rational set of mechanisms for classification and declassification, the skewed incentive structure underlying the system tends to feed massive overclassification. The words of the Moynihan Committee still ring true today: "Any policy, including on classification and declassification, is only as good as its implementation."[249]

IV. A PROPOSAL TO REDUCE OVERCLASSIFICATION

The previous chapter identified the skewed incentive structure that underlies the current classification system and promotes overclassification. This chapter proposes a multi-pronged solution designed to rebalance the operative incentives, primarily by introducing accountability for classification decisions at the individual and agency level.

In the 1990s, the Moynihan Commission reported that "[a]ccountability should be a hallmark of a well-functioning secrecy system …. We therefore recommend improving training and enhancing incentives so that classifying officials will consider more carefully the costs of secrecy and recognize that they will be accountable for their decisions."[250] This chapter proposes a system under which classifiers would detail their reasons for classification, have those decisions audited, and face sanctions for severe or recurring overclassification. Senior-level managers would be held accountable for chronic poor performance by their employees, and agencies would be required to devote imagination and resources to the problem of reducing overclassification. Agencies also would be required to dedicate more resources to training programs and to obtain ISOO approval of training materials. Derivative classifiers would be protected against sanctions for failing to classify information in cases where the original classifier's guidance was ambiguous. Finally, incentives would be offered to authorized holders who successfully challenged the improper or erroneous classification of information. Together, these measures would begin to correct the imbalance of incentives that sustains the current overclassification problem.

We propose a multi-pronged solution designed to correct the imbalance of incentives that sustains the current overclassification problem.

We recommend that this proposal be implemented as a pilot program within one or two agencies.[251] This would allow a study of the proposal in operation to confirm that its benefits outweigh its costs, that there are no unanticipated consequences, and—most fundamentally—that it is successful in reducing overclassification. This observation and analysis should be conducted by ISOO over a period of two to three years. The test agency or agencies should be required to collect and furnish any information ISOO deems necessary for this process, and the result of ISOO's review should be made public.

In measuring the costs and benefits of the proposal, certain key points must be considered. First, the proposal would require an initial outlay with respect to establishing the computer programs, audit systems, and personnel practices discussed below. The costs of the proposal, in other words, would be somewhat front-loaded, while the benefits would accrue over time. Second, many of the benefits, as well as some of the costs, would be difficult to quantify. Certainly, any decline in the amount that an agency spends on classification can be measured—albeit not with complete precision.[252] Similarly, one can measure the number of classification decisions originating from an agency, as well as changes in the amount of overclassification (as determined through the audits discussed herein); indeed, these would be key measurements. But there is no way to quantify the value of enhanced democratic decision making, nor is there any way to quantify the "hassle factor" for classifiers who would be required to put more time and thought into their decisions. Ultimately, the decision whether to expand the pilot program would be a matter of informed judgment rather than mechanistic calculation.

If done as a pilot project in one or two agencies, much if not all of our proposal could be implemented through executive order and accompanying ISOO directive, even though legislation might be required to implement the proposal government-wide.

A. Use of Electronic Forms

One of the primary "enablers" of overclassification, as discussed above, is the ease and lack of reflection with which classifiers may block information from entering the public sphere. To address this problem, we propose that the President amend his executive order to require classifiers to "identify and describe the damage" they are seeking to prevent through classification, rather than simply being "*able to* identify and describe the damage."[253] To this end, ISOO would develop short questionnaires (detailed below) that classifiers would have to complete and that would require them to provide, in addition to the basic information that is currently required, a narrative explanation of the reasoning behind their decisions.

As virtually all classified documents are now created electronically, with classifiers marking e-mails and documents using drop-down features in computer programs, classifiers generally would answer the questions by responding to electronic prompts, rather than by completing a paper form. Technology thus would be harnessed to promote reflection rather than to obviate the need for it, as is often the case now. The answers to the drop-down questions would become part of the document's metadata (i.e., the structured information that describes the format, content, context and organization of the underlying information in an electronic document or record[254]) and would follow the document throughout its classified lifespan.

Some flexibility would be required to ensure that the process of completing the electronic forms would not interfere with the business of government or national security. Government officials often generate classified documents under exigent or time-sensitive circumstances, such as planning military operations slated to occur only days or hours in the future. Officials should therefore have the power to classify documents on an interim basis—for no more than ten days—without completing the full form. They could instead certify (in response to the first electronic prompt) that they were classifying the document under particularly urgent or time-sensitive conditions; this certification would allow them to bypass the questions requiring a narrative response and provide only the basic information currently required of classifiers. They would then have ten days (and would receive automatically-generated e-mail reminders of this deadline) to return to the document and complete the remaining questions. If they failed to do so, the information would lose its classified status.

In addition, because requiring each participant in an e-mail thread to re-justify the thread's classification would be inefficient and overly burdensome, a different system would be required for e-mails. The originator of a classified e-mail would be required to complete an electronic form. If the recipient(s) hit "reply," a drop-down prompt would ask whether the reply e-mail contained new information (i.e., information not substantially the same as the information in the originating e-mail) that required classification. Only if the reply e-mail contained new information would the sender be required to complete another full questionnaire.

The electronic forms would have several advantages. First, and most important, requiring classifiers to articulate the justification for classifying a document would help ensure that such justification actually exists. As the Moynihan Commission found, "Requiring … a written justification would prompt original classifiers to think more carefully about their decisions."[255] A well-intentioned classifier who was inclined to classify a document out of mere habit or expediency, and who lacked any compelling national security rationale for doing so, would likely abandon the exercise rather than engage in an affirmative deception. Similarly, a classifier who was inclined to classify a document based only on a vague (but good faith) sense that certain information is the "type" of information that generally should be classified would be pressed to give the decision more thoughtful consideration.

Of course, there would be the potential for classifiers to develop a series of "boilerplate" answers that they could draw upon when classifying particular types of documents. But even this would require a greater degree of reflection than, and therefore would be preferable to, the current system. After all, if the boilerplate answers were too vague or were applied in inapplicable circumstances, the classifier would risk an adverse audit result (as discussed below).

Second, the process of completing the form would constitute an administrative burden, albeit a small one, on those who classify documents. Some readers of this report will surely criticize the proposal on that basis. Yet the creation of a *minimal* burden—the forms would not require extended essays, and at bottom, the thought process they would require is one classifiers already are required to undertake—is not only justified by the increased accountability the process would provide; it would in fact be a salutary effect of the proposal. In a democracy that relies on an informed public for effective self-government, removing information from the public sphere, often for a period of many years, is a momentous thing. It should be treated as such—not as a casual administrative function. Indeed, it is difficult to imagine any other government action that so seriously affects the rights of the people that is not subject to a panoply of procedural protections. More concretely, while the forms we propose are designed not to be overly burdensome, the time and effort required to complete them might nonetheless be sufficient to dissuade those classifiers whose only rationale for classifying a document is: "Why not?"

A third advantage is to provide a basis on which reviewers can audit classifiers' decisions (as proposed below). Without knowing why a classifier chose to classify a particular document, the auditor would be required to study the document, posit all of the possible reasons why the information in the document *might* jeopardize national security, and then evaluate those reasons. Particularly if the auditor were not immediately steeped in the document's subject matter, this could mean a difficult and time-consuming process of reinventing the wheel. On the other hand, if the classifier were to provide sufficiently clear reasons for classifying a document, only a brief review of the document itself (and the relevant source document(s) or classification guide, in the case of a derivative classification) might be necessary for the auditor to evaluate the decision.

Fourth, incorporating the answers to the questionnaires into documents' metadata would prove useful in a variety of ways. For one thing, derivative classifiers would be able to see the original classifier's rationale for classifying a document, which might assist them as a general matter in their own classification decisions. In addition, there are a variety of administrative uses for metadata. For example, metadata indicating the date on which a particular document should be declassified could be used to effectuate

the document's automatic declassification; metadata specifying the paragraph of an agency guide authorizing classification could be used to declassify documents or flag them for review if that paragraph were subsequently removed or revised; and metadata identifying the source document for derivative classification decisions could be used to declassify derivatively classified documents automatically when the source document was declassified.

1. Electronic Forms for Original Classifiers

We propose that original classifiers be required to complete an electronic version of the model form on the following page (Model Form – Original Classification).

Questions 1 through 4 would solicit basic information required under the executive order and implementing directive: the overall classification level of the document (to include any special dissemination control or handling markings); the name and position or personal identifier of the classifier; the agency and office of origin; and the date of origin of the document.[256]

Question 5 would require the original classifier to "identify or describe the damage to national security that disclosure of this document could cause," and to "explain why classification at the designated level (Confidential, Secret, or Top Secret) is warranted." This question flows from the executive order's definitions of the various levels of classification[257] and from the requirement that an original classifier must determine that "the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security … and the original classification authority is able to identify or describe the damage."[258]

Question 6 would require the original classifier to "identify the applicable category or categories of information under Section 1.4 of Executive Order 13,526 and explain why the category or categories apply." This question reflects the requirement that classified information "pertain[] to one or more" of the categories of information specified in Section 1.4 of the executive order.[259]

The various parts of Question 7 would require the original classifier to certify compliance with other provisions of the executive order. Making these certifications would place some pressure on the classifier to consider the accuracy of what he or she was certifying. For example, the classifier would have to certify that "[t]he purpose of classifying this document is not to conceal violations of law, inefficiency, or administrative error," to "prevent embarrassment to a person, organization, or agency," to "restrain competition," or to "prevent or delay the release of information that does not require protection in the interest of national security," tracking Subsections (a)(1)-(4) of Section 1.7 of the executive order.[260] The classifier similarly would have to certify compliance with the executive order's requirement that "the classification authority shall, whenever practicable, use a classified addendum whenever classified information constitutes a small portion of an otherwise unclassified document or prepare a product to allow for dissemination at the lowest level of classification possible or in unclassified form."[261]

Question 8 would require the original classifier to specify a date or event for declassification, as required by Section 1.5(a) of the executive order.[262] In keeping with the provisions of Section 1.5(b), a classifier who chose a ten-year time frame would have to certify that he or she could not determine an earlier date

MODEL FORM – ORIGINAL CLASSIFICATION

1. Classification level: _____

2. Classified by: _____

3. Agency and office of origin: _____

4. Date of origin of document: _____

5. Identify or describe the damage to national security that disclosure of this document could cause, and explain why classification at the designated level (Confidential, Secret, or Top Secret) is warranted.

6. Identify the applicable category or categories of information under Section 1.4 of Executive Order 13,526 and explain why the category or categories apply.

7. I hereby make all of the following certifications:

❑ The purpose of classifying this document is not to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent the delay or release of information that does not require protection in the interest of national security.

❑ I have no significant doubt that this document needs to be classified and no significant doubt as to whether it should be classified at this or a lower level.

❑ Classified portions of this document do not contain basic scientific research information, unless such information is clearly related to the national security.

❑ I have marked each portion of the document as unclassified or with the appropriate classification level, **OR** ❑ the Director of the Information Security Oversight Office has granted a waiver of this requirement.

❑ I have used a classified addendum; **OR** ❑ I have prepared a product to allow for dissemination at the lowest level of classification possible or in unclassified form; **OR** ❑ I did not prepare a product to allow for dissemination at the lowest level of classification possible or in unclassified form because doing so would be impracticable, and I did not use a classified addendum because ❑ it is not the case that classified information constitutes a small portion of this document, or ❑ using a classified addendum would be impracticable.

8. Specific date or event for declassification: _____

8(a). *To be completed for classification for 10 years:* ❑ I hereby certify that I cannot determine an earlier specific date or event for declassification.

8(b). *To be completed for classification for over 10 years:* This document requires classification for the period specified in Question 8 because:

8(c). *To be completed for classification for over 25 years:*

❑ I hereby certify that this document should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction.

I hereby certify that all responses above are true to the best of my knowledge, information, and belief.

_____ _____

Signature Date

or event for declassification, while a classifier seeking to classify a document for more than ten years would have to explain why the information required extended classification.[263] If classification would exceed twenty-five years, the classifier would have to certify that the information "should clearly and demonstrably be expected to reveal the identity of a confidential human source or a human intelligence source or key design concepts of weapons of mass destruction," as provided in Section 1.5(a).[264]

2. Electronic Forms for Derivative Classifiers

Derivative classification, in theory, should be a ministerial act of carrying forward an original classifier's decision. As discussed above, however, some agency classification guides contain broad standards that require derivative classifiers to make judgment calls similar to those made by original classifiers. Unless and until agency classification guides are revised to eliminate this element of broad discretion (President Obama's order that agencies conduct a "fundamental classification guidance review" may help in this regard),[265] derivative classifiers, when classifying information based on guides, should be required to document their reasoning. Moreover, all derivative classifiers should be presented with a drop-down prompt that requires them to identify the original classification decision (whether reflected in a guide or a source document) that justifies derivative classification, in order to address the problem of derivative classifiers wrongly believing that they have independent authority to classify information.[266]

We propose the model form on the following page for derivative classifiers working from an agency classification guide (Model Form – Derivative Classification From Guide).

Questions 1 through 4 would request the same basic information as the first four questions on the model form for original classifiers.

Question 5 would require the derivative classifier to specify the classification guide, and the particular paragraph of the guide, that provides the basis for classification. The current implementing directive allows a derivative classifier to cite the entire guide, rather than the relevant paragraph.[267] Such a general citation allows derivative classifiers to classify documents without thinking through the specific basis for classification. Question 5 also would require the derivative classifier to provide an explanation, in narrative form, of why the document meets the criteria in the specified paragraph of the guide.

Question 6 would require the derivative classifier to state the duration of classification, and to explain why the classification guide justifies such a duration (again, some classification guides give derivative classifiers a significant amount of discretion in this area).[268] Question 7 would require derivative classifiers to certify their compliance with the provisions of the executive order and implementing directive that mandate the use of portion markings and classified addendums,[269] as well as the truthfulness of their answers to all questions on the form.

In contrast to derivative classification from guides, which can involve a great deal of discretion, derivative classification from source documents represents a straightforward process in which classifiers transfer markings from previously classified documents. Accordingly, it is not necessary for derivative classifiers to provide narrative explanations for such decisions. Derivative classifiers should, however, be prompted to specify the source documents on which they rely, as required by the executive order and

MODEL FORM – DERIVATIVE CLASSIFICATION FROM GUIDE

1. Classification level: _____

2. Classified by: _____

3. Agency and office of origin: _____

4. Date of origin of document: _____

5(a). I have classified this document based on paragraph(s) _____ of the following classification guide: _____

5(b). Explain why the document meets the criteria for classification under the paragraph(s) specified in response to Question 5(a).

6(a). Specific date or event for declassification: _____

6(b). The time period specified in response to Question 6(a) is compelled by the paragraph(s) of the classification guide identified in response to Question 5(a) for the following reasons:

7. I hereby certify:

❑ I have marked each portion of the document as unclassified or with the appropriate classification level, **OR** ❑ the Director of the Information Security Oversight Office has granted a waiver of this requirement.

❑ I have used a classified addendum; **OR** ❑ I have prepared a product to allow for dissemination at the lowest level of classification possible or in unclassified form; **OR** ❑ I did not prepare a product to allow for dissemination at the lowest level of classification possible or in unclassified form because doing so would be impracticable, and I did not use a classified addendum because ❑ it is not the case that classified information constitutes a small portion of this document, or ❑ using a classified addendum would be impracticable.

❑ All responses above are true to the best of my knowledge, information, and belief.

_____ _____

Signature Date

implementing directive.[270] Classifiers relying on multiple sources would be prompted to enter a list of the source materials. This would track the current executive order and implementing directive, under which derivative classifiers may enter the phrase "multiple sources" on the "Derived By" line but must include a list of those sources on or attached to the document.[271] In addition, derivative classifiers would be prompted to certify compliance with the portion marking and classified addendum requirements of the executive order and implementing directive. These questions and certifications are reflected in the model form on the following page for derivative classifiers working from source documents (Model Form – Derivative Classification From Source Documents).

B. Office of Inspector General Audits

We propose that the President issue an executive order directing the creation of a system to audit classification decisions at one or two test agencies. While completing electronic forms would promote deliberate decisions, forms alone would not ensure that classifiers exercise their authority responsibly. Audits would provide a backstop to the forms, making sure that classifiers give adequate reasons and helping to deter abuses and correct erroneous decisions—in short, introducing accountability into the classification process.

In addition, audits would help ensure that the improvements contained in the December 2009 executive order are realized. For example, the order contains a requirement that classifiers refrain from classification if there is "significant doubt" regarding the need to classify.[272] In theory, this provision should change the default in cases where classifiers are uncertain about the need to classify, which could in turn lead to a substantial reduction in overclassification. In practice, however, the incentives that currently promote classification in such cases—the culture of secrecy among certain agencies, fear of sanctions for "underclassifying," and the press of business—are likely to prevail unless classifiers are held accountable for their adherence to the new rule. President Obama's executive order also requires derivative classifiers to identify themselves on documents that they classify.[273] This requirement will make it possible, for the first time, to hold derivative classifiers accountable for mistakes or abuses—but only if there is a system in place for assessing their performance.[274]

The audits that we propose would include review of classification decisions for both substantive correctness and compliance with procedural requirements (including proper completion of the proposed electronic forms). While the purpose of the review is to identify instances of overclassification, failure to comply with procedural requirements can itself cause overclassification and is therefore an appropriate subject of review. For example, if a classifier fails to portion mark a document, the classification level given to the entire document—which reflects the classification level of the most sensitive information within that document—will be applied to all of the information therein, including information that could be classified at a lower level or publicly released. Similarly, the failure to specify a date or event that should trigger declassification could well result in the information remaining classified long after it loses its sensitivity. And the failure to use a classified addendum affects the availability, if not the actual classification status, of the unclassified information in a given document.

Within each agency, the audits would be performed by personnel in the agency's Office of the Inspector General (OIG). The OIGs are the proper bodies to conduct these audits because of their independence

MODEL FORM – DERIVATIVE CLASSIFICATION FROM SOURCE DOCUMENTS

1. Classification level: _____

2. Classified by: _____

3. Agency and office of origin: _____

4. Date of origin of document: _____

5(a). Derived From: _____

5(b). *To be completed if "multiple sources" was entered in response to Question 5(a):* Provide a complete list of the source materials.

6. Specific date or event for declassification: _____

7. I hereby certify:

❑ I have marked each portion of the document as unclassified or with the appropriate classification level, **OR** ❑ the Director of the Information Security Oversight Office has granted a waiver of this requirement.

❑ I have used a classified addendum; **OR** ❑ I have prepared a product to allow for dissemination at the lowest level of classification possible or in unclassified form; **OR** ❑ I did not prepare a product to allow for dissemination at the lowest level of classification possible or in unclassified form because doing so would be impracticable, and I did not use a classified addendum because ❑ it is not the case that classified information constitutes a small portion of this document, **OR** ❑ using a classified addendum would be impracticable.

❑ All responses above are true to the best of my knowledge, information, and belief.

_____ _____

Signature Date

within the agencies. Congress has mandated that Inspectors General be appointed "without regard to political affiliation," and while they report to the heads of the agencies or the second-ranking agency officials, they are not subject to supervision by any other agency personnel and can be removed only by the President (or, in the case of certain specially designated federal entities, the agency head or governing board).[275] The audits accordingly would not suffer the same problems as the agency self-inspection programs,[276] which have foundered, according to repeated observations by ISOO, on lack of support from agencies' senior management.[277] Nor would the possibility of ideological or political resistance to the audit process be likely to arise, as it might if the audit responsibility were assigned to the political head of one or more relevant agencies. The suitability of the OIGs to perform this role is buttressed by the recently enacted Reducing Over-Classification Act, in which Congress charged the OIGs with the task of assessing their agencies' compliance with "applicable classification policies, procedures, rules, and regulations."[278] (Congress's mandate is not a substitute for the audits proposed herein because Congress did not require OIGs to review individuals' classification decisions as part of their evaluations.)

Spot audits of classifiers would help to deter abuses and correct erroneous decisions—in short, introducing accountability into the classification process.

Wherever possible, the OIGs would undertake to audit every original classifier within their agencies each year. For those agencies in which the number of original classifiers would make such a comprehensive audit impracticable, the OIGs would conduct a "spot audit" of randomly chosen original classifiers. Similarly, because the number of derivative classifiers is too large to permit a yearly audit of all of them, the OIGs would spot-audit a randomly selected cohort of derivative classifiers each year. While such spot audits would not catch misuse of classification authority among those classifiers who were not audited in a given year, they might help to prevent such misuse in the first place, as the potential for an audit and sanctions could be expected to prompt better compliance with the rules.

For each classifier being audited, OIG personnel would review a random sample—comprising perhaps 20-30 documents—of that individual's classified product. As noted above, the electronic forms would greatly facilitate the document review because the auditor would be able to evaluate the stated reason for classification, rather than guessing at the classifier's justification. In many cases, the review would constitute a straightforward process of comparing the information provided on the form to the information contained in the classified document and (for derivative classification decisions) the relevant source document(s) or agency classification guide. However, as with other OIG inspections, agencies would be required to afford the OIGs access to any additional information—including access to agency personnel—necessary to conduct a thorough evaluation.[279] If the initial audit of a classifier raised concerns, the auditor could review additional documents to confirm that assessment.

If a sufficient number of randomly chosen classifiers were audited, the OIG at each agency would be able to use the audits to assess the agency's overall performance, including an estimate of the rate of overclassification agency-wide. This information would be set forth in an annual report to the agency and to Congress, which would be issued in unclassified form and made available to the public. In addition, the results of the individual audits would be forwarded to appropriate agency personnel in order to effectuate the consequences discussed in the next section.

A few points with regard to the involvement of the OIGs should be noted. First, while the President or the heads of agencies may *request* that OIGs conduct particular investigations, only Congress can *require* them to do so.[280] We have recommended that our proposal be implemented as a pilot project at one or two agencies, and the President should select those agencies based in part on which OIGs are amenable. Implementing the proposal government-wide, however, likely would require legislation. Government-wide implementation also would require the amendment of statutes that currently allow some agencies to exercise control over, and in some cases block, OIG audits or investigations with national security implications.[281] And, in cases where an office that engages in classification does not have an OIG (for example, the Office of the Vice President), Congress should enact a statute enabling the President to designate officials to conduct the audits and providing funding for such officials and their staff.

Second, it is important that the approaches employed by the various OIGs be uniform to the extent possible, both to ensure confidence in the results and to enable a comparison of the agencies. Accordingly, ISOO should issue a directive providing the OIGs with guidance on how to conduct audits, and it should provide training to the OIGs at least once every two years. While ISOO itself does not have the resources to conduct audits in every agency, it has historically conducted a type of audit similar to the one proposed here, visiting a small number of agencies each year and examining a sample of each agency's classified product in order to assess the agency's overall performance.[282] It therefore would be well-positioned to counsel the OIGs.

Third, the OIGs might require assistance on some substantive questions. They should easily be able to detect the type of procedural irregularities (such as failure to use portion markings or to specify the original classification decision underlying a derivative classification) that plague such a high proportion of classified documents. Moreover, the use of the forms discussed above should in most cases enable OIGs to assess whether the classifier has articulated a facially valid national security reason for a given document's classification. To be sure, OIGs might lack the substantive expertise to spot weaknesses in justifications that appear legitimate to a layperson, and might therefore err on the side of the classifier. Nonetheless, they should be able to spot flagrant misuses of the classification system. For those cases that fall in the middle—i.e., there is no obvious error or abuse, yet the justification provided by the classifier raises questions—ISCAP could serve in a consulting role, advising the OIG on whether classification of the document was appropriate.[283]

C. Consequences for Improper Classification Practices

The OIG audits proposed above would help develop a better understanding of the scope and nature of the government's overclassification problem. But the primary purpose of the audits is functional rather than academic: to reduce overclassification by introducing accountability into the system. In order to achieve this result, the findings of the audits must be tied to mandatory consequences for the individual classifier and (in some cases) agency supervisors and even the agency itself. Without such consequences, there will be no accountability, and the incentives to overclassify will continue to dwarf the disincentives.

1. Consequences for Individual Classifiers

If an audit raised concerns about a classifier, the auditor would inform the classifier and identify the errors that the he or she had made. The auditor would schedule a second audit of the classifier six months

later. If the second audit showed continuing problems, this would trigger additional semiannual audits and a series of escalating consequences.

Of course, the judgment underlying original classification decisions (and some derivative ones) is ultimately a subjective one, and reasonable people with equal knowledge of the subject matter may reach different conclusions about whether a given document should be classified. Indeed, ISCAP, which decides classification appeals by majority vote, is not infrequently divided in its decisions.[284] Executive Order 13,526's new requirement that classifiers refrain from classifying documents if significant doubt exists should significantly narrow the permissible grey area, but may not eliminate it entirely. Accordingly, disagreement with a classifier's decision in a small number of cases should not be sufficient to trigger repeat audits and their attendant consequences. Instead, follow-up would occur if (a) the classifier ignored procedural requirements (which involve no element of subjective judgment); (b) the auditor determined that the classification decision was substantively erroneous or unsubstantiated more than 25 percent of the time (a rate that would allow a comfortable margin for mere differences in opinion); and/or (c) the auditor determined that, in one or more cases, the classifier classified a document for a prohibited purpose—e.g., to conceal government wrongdoing or misconduct.

Classifiers who, after being found deficient in their performance, continued to overclassify or otherwise failed to comply with classification requirements would face escalating consequences, to be spelled out in ISOO directive and agency regulation. Such consequences would begin with an intensive course of remedial training. Remedial training would be followed, in the event of poor performance on the next follow-up audit, by a negative report in the classifier's personnel file. Next, a classifier would be subject to temporary suspension of his or her classification authority; the period of suspension could be lengthened for subsequent infractions. The series of consequences would culminate, where necessary, in permanent revocation of the individual's classification authority.

Such sanctions would serve two purposes. First, employees who routinely engage in overclassification not only are ignoring the direction of the President and the agencies for which they work; they are putting the security of the nation in jeopardy by contributing to a problem that greatly undermines the efficacy of the classification system. Ensuring that these employees do not continue to overclassify would ultimately strengthen the government's information security practices. Second, the ability to classify information is generally a critical element of the jobs held by those who have classification authority. Indeed, because the ability to classify derivatively is essential to protecting the security of already-classified information, suspension or revocation of classification authority could effectively preclude the individual from working with classified information in any capacity. Loss of classification authority is thus a uniquely meaningful sanction, and the threat of its application would provide a powerful incentive for employees to be more careful in their classification decisions—which, over time, would ideally obviate the need for the sanction to be used at all.

2. Consequences for Agencies and Senior Management

As discussed above, a primary culprit behind the problem of overclassification is the culture of secrecy that exists among many of the agencies that produce the most classified information. In general, the culture of an organization is highly dependent on the attitudes and priorities of the organization's

leadership. Accordingly, while attaching consequences to employees' improper use of classification authority may influence behavior at the individual level, it is unlikely to influence the overall culture of the agency, even if it provides an important counterweight to that culture. Instead, those who study organizational culture change agree that such change must come from the top down.[285]

Unfortunately, although the executive order states that agency heads must "demonstrate personal commitment," "commit senior management," and "commit necessary resources" to the successful and effective implementation of the classification system,[286] such exhortations are seldom realized on the ground. As the Moynihan Commission observed, "responsibility for ensuring judicious classification rests almost entirely within individual agencies, which rarely view reducing classification as a priority."[287]

An exception—and a key illustration of the importance of agency leadership—is the case of Hazel O'Leary, who served as Secretary of the Department of Energy under President Clinton. Reportedly motivated by personal horror at the classified radiation experiments conducted on human subjects during the Cold War, Secretary O'Leary in 1995 undertook a major effort to revise the department's classification guides, with the stated goal of reducing classification.[288] This process, known as the Fundamental Classification Policy Review, was widely viewed as a major success[289] and ultimately declassified the complete list of U.S. nuclear explosive tests, as well as information on the history of U.S. production of plutonium and highly enriched uranium.[290]

Ideally, the President would appoint leaders of agencies, like Secretary O'Leary, who are personally committed to reducing overclassification. In practice, however, the President is unlikely to give this criterion significant weight in appointing agency heads: it would make little sense for those agencies that engage in relatively little classification, and it would generally be outweighed by other considerations—primarily, that of foreign policy, military, or intelligence expertise—for those agencies, like the CIA or Defense Department, that produce large volumes of classified information.

Accordingly, we propose that incentives be put in place to help motivate the leadership of these agencies, once appointed or hired, to promote sound classification practices among employees. Instilling such practices would become a part of senior managers' job descriptions and performance evaluations. In particular, managers would be held accountable for correcting the performance of employees under their supervision who were found, during the OIG audit process, to be classifying documents improperly. If the employees of a particular supervisor persistently engaged in overclassification or failed to respect procedural requirements, this fact would be reflected in the manager's personnel evaluation and would affect his or her eligibility for bonuses and other performance-related benefits.

Moreover, just as individual classifiers would be held accountable for their own performance and managers would be held accountable for the performance of the employees they supervise, agencies would be held accountable if the OIG audits suggested an agency-wide overclassification problem that the agency failed to correct over time. If, in a given year, an audit revealed problems with a high percentage (e.g., more than 25 percent) of the classified documents examined at a particular agency, this fact would be included in ISOO's annual report to the President. If the agency in question failed to significantly reduce that percentage the following year, it would be required to devise a comprehensive plan to reduce the rate of improper classification by a fixed amount over a fixed period of time (the

amount and time period would depend on the agency and the extent of the problem). The agency's plan would have to demonstrate that it was committing the resources and personnel necessary to effectuate its strategy.

ISOO would be responsible for reviewing and approving agency plans. If ISOO found an agency's plan to be insufficient, it would have the authority to direct revisions. Approved plans would be submitted to the President. Agencies would be required to submit annual follow-up reports; if subsequent OIG audits showed that an agency's plan had failed to accomplish the target reductions in the proportion of documents improperly classified, the agency would have to explain the failure and, if so directed by ISOO, propose revisions to its plan (including the dedication of additional resources where necessary).

D. Improvements to Training Programs

Because a pattern of overclassification would subject classifiers to serious consequences under this proposal, it would be all the more important that classifiers receive adequate training in proper classification practices. President Obama's executive order for the first time requires that original and derivative classifiers receive training on avoiding overclassification; indeed, it prohibits them from classifying documents if they do not receive such training every year (for original classifiers) or two years (for derivative classifiers).[291] This is among the most important improvements contained in President Obama's order. If faithfully implemented, a rigorous training requirement would not only reduce instances of overclassification; it could even begin to chip away at the culture of secrecy that pervades so many of the relevant agencies.

In order to fulfill the promise of this new requirement, however, agencies must do a better job of conforming their training programs to the requirements of the executive order and implementing directive—an area in which they consistently have fallen short in the past.[292] To that end, we propose two new measures.

The first measure would increase the resources agencies devote to training programs. ISOO has attributed the shortcomings in agencies' training programs to insufficient resources—in particular, insufficient security staff.[293] As discussed in Chapter 1, agencies spent more than 10 billion dollars on security classification in fiscal year 2010 (and this figure does not include agencies, such as the CIA, that classify their classification budgets). But agencies spend very little on classification training, and devoted less than 4% of their security classification budgets to such training in fiscal year 2010.[294]

Additional appropriations for classification training are unlikely in the current fiscal climate. A rebalancing of agencies' existing classification budgets, on the other hand, would be not only feasible but desirable: if agencies spend more money on training, there will be less overclassification,[295] and agencies consequently will spend less money protecting information that could safely be disclosed. Accordingly, we propose that the Office of Management and Budget (OMB) direct agencies to spend a minimum of eight percent of their classification budgets on training. If an agency consistently performed poorly on OIG audits, OMB could direct that a higher percentage be devoted to training until the audits revealed significant improvement.

The second measure would require agencies to submit their training materials to ISOO for approval and to make any necessary changes to those materials as directed by ISOO, on the same terms that ISOO now approves agencies' implementing regulations.[296] ISOO would not approve training materials unless they included appropriate instruction in the agency guides used by derivative classifiers, as these guides, in combination with source documents, establish the limits of derivative classifiers' authority. This would give substance to the executive order's requirement that agencies provide training in avoiding overclassification, and it would ensure that trainings give equal and appropriate weight to both the protection of classified information and the proper use of the classification system.

E. "Hold Harmless" Rule for Derivative Classifiers Acting Without Clear Guidance

As discussed above, the lack of any consequences for needless classification contrasts sharply with the all-too-real prospect of reprimand or official sanction for failure to protect sensitive information. Providing a mechanism to hold classifiers accountable for overclassification would begin to address this imbalance in incentives. However, if classifiers who were subject to audits and accountability for overclassification were simultaneously threatened with sanctions if they were perceived to be *underclassifying*, they might feel trapped between a rock and a hard place. As the Chair of the Public Interest Declassification Board put it at a recent public meeting, classifiers need to "feel safe" to do the right thing.[297]

A "hold harmless" rule in cases where classification is not clearly required would alleviate one potent source of pressure to overclassify.

The notion of sanctions for "underclassification" is problematic in many respects. It is an often-overlooked fact that the executive order does not *require* the classification of information in the first instance (i.e., by an original classifier), even if that information meets the relevant criteria. Instead, the order provides that "[i]nformation *may* be originally classified under the terms of this order . . . if all of the following conditions are met."[298] An original classifier may determine that information is eligible for classification, but that considerations of policy, strategy, or public interest outweigh the risk to national security. A former head of ISOO has indeed encouraged original classifiers to focus more on the question of whether documents *should* be classified (and not just whether they *can* be classified),[299] and the Public Interest Declassification Board has solicited public comment on a proposal to encourage discretionary release of information that qualifies for classification.[300] Given this element of discretion, sanctioning an original classifier for a decision not to classify information would rarely be appropriate absent bad faith or clear negligence.

By contrast, the executive order clearly states that derivative classifiers "shall . . . observe and respect original classification decisions."[301] In theory, adherence to this mandate should be a straightforward matter, as the classified portions of source documents should be clearly marked, and agency classification guides should describe categories of classified information with sufficient precision to eliminate any guesswork. In practice, however, the decision whether to apply derivative classification is often far from clear. As noted above, some classification guides are so vague that they essentially deputize derivative classifiers to make original classification decisions. Furthermore, classified information may be conveyed

orally as well as in writing, in which case it may come without clear "markings" to guide the derivative classifier in re-transmitting the information.

In the absence of a clear indication that specific information has been deemed classified by an original classifier, derivative classifiers arguably should err against classification, as they lack authority to classify information on their own. In fact, however, the fear of repercussions for failing to "observe and respect original classification decisions" leads derivative classifiers to default to classification, lest they be penalized for guessing wrong.

We propose a "hold harmless" rule under which derivative classifiers would not be held responsible for failing to follow original classification decisions when those decisions were not clearly conveyed. Through executive order, the President would specify that derivative classifiers may not be subject to reprimand, sanctions, or any other negative consequence for failure to classify information unless classification of the specific information in question was unambiguously required by virtue of (1) a properly marked source document; (2) a current classification guide that was provided to the classifier, along with appropriate training in its contents; or (3) express identification of the information's classified status (in the context of oral transmission of information). A similar "hold harmless" rule would provide that original classifiers may not be subject to reprimand, sanctions, or any other negative consequence for reasonable, good-faith decisions not to classify documents that meet the criteria for classification. The prohibition would specify that the prohibited negative consequences would include restrictions on classification authority and suspension or revocation of clearances.[302]

Derivative classifiers would remain subject to sanctions, and appropriately so, if they knowingly, willfully, or negligently failed to respect original classifiers' *unambiguous* determinations. Moreover, all classifiers would remain responsible for protecting against unauthorized disclosure of classified information. The proposed rule accordingly would not threaten the security of properly classified information; it would simply alleviate one potent source of pressure to err liberally on the side of classification in cases where classification is not, or might not be, appropriate. And it would have the salutary effect of encouraging clarity and specificity in original classification decisions and agency classification guides.

F. Incentives to Challenge Improper Classification Decisions

Authorized holders who come across needlessly classified documents have the perfect vantage point for challenging the decision to classify, and the executive order states that they are "encouraged and expected" to raise such challenges.[303] As discussed above, however, such challenges rarely occur because many authorized holders do not know they can bring them; even if they are aware of the provision, they lack any incentive to dedicate the time and effort required; and the system for bringing challenges does not take into account the pressure from supervisors and peers not to challenge colleagues' classification decisions.

We propose three ways to invigorate classification challenges. First, agencies would be required to institute a process by which authorized holders could bring challenges anonymously, and to include information about this process in their classification training. ISOO would not approve training materials that lacked detailed information about the process for bringing challenges.

Second, in order to give authorized holders an incentive to challenge wrongful classification decisions, agencies would be required to award small cash prizes for those who bring successful challenges.[304] Anonymous challenges would be assigned a unique identifier that would enable challengers to track the status of their challenges and to claim any reward. Prizes on the order of $50 for a successful challenge at the agency level and $100 for a successful appeal to ISCAP—with a cap on the total amount that could be awarded to any single challenger in a given year—could create an incentive for such challenges without requiring any major expenditure. Such prizes could fall under the existing statutory authorization for Presidential or agency awards for "a special act or service in the public interest."[305] (Along similar lines, the Reducing Over-Classification Act encourages the President and federal agencies to consider an employee's "consistent and proper classification of information" in determining whether to award any personnel incentive.[306] The OIG audits described in this report could be used to identify employees who are eligible for this statutory benefit, which otherwise might be difficult to operationalize.)

Finally, in order to eliminate concerns that a more robust system of challenges might undermine *esprit de corps* in agencies or components where such an atmosphere is important to mission success—and to address the related problem of employees not bringing challenges because they don't want to subject their colleagues to disciplinary action—the rules for bringing challenges would specify that successful challenges could not trigger sanctions against the classifier unless the classification decision appeared to reflect a willful or egregious violation of classification requirements.

• • •

The incentive structure underlying the problem of overclassification is deeply entrenched, but it is not immutable. Each of the proposed changes in this chapter would promote more careful and principled decisionmaking on the part of classifiers. Together, these proposals hold the potential for tipping the balance of incentives and significantly reducing overclassification.

CONCLUSION

From the early days of the Cold War, when the government classified information to hide the truth about human radiation experiments and a congressional subcommittee found that examples of overclassification "ranged from the amusing to the arrogant,"[307] to the current struggle against terrorism, in which overclassification has become a "barrier (and often an excuse) for not sharing pertinent information with homeland security partners,"[308] needless secrecy has reigned, despite efforts to curb it. Checks against overclassification have proven insufficient, and proclamations made on paper have failed to take hold on the ground.

On his first full day in office, President Obama directed agencies "to usher in a new era of open Government,"[309] and at the end of last year, he revised, for the better, the executive order at the pinnacle of the classification system. But more remains to be done in order to bridge the gap between exhortation and reality. By implementing a pilot project along the lines proposed in this report and introducing accountability into the system, the government can begin to change the incentives that have produced overclassification for so many decades. The result will be a more transparent government and a better-functioning democracy.

ENDNOTES

[1] The term "overclassification" is used differently in different contexts. In some contexts, it is used to signify the classification of information at a higher level than the information warrants—e.g., classifying a document as "Top Secret" when it is more appropriately classified as "Confidential." In other contexts, the term is used to signify classification of documents that do not warrant classification at all. This report uses the term primarily in the latter sense.

[2] Nat'l Comm'n on Terrorist Attacks Upon the U. S., The 9/11 Commission Report: Final report of the National Commission on Terrorist Attacks Upon the United States 417 (2004) [hereinafter 9/11 Commission Report].

[3] *Mark-up of Fiscal Year 1994 Foreign Relations Authorization Act: Hearing Before the Subcomm. on Terrorism, Narcotics and Int'l Operations of the S. Comm. on Foreign Relations*, 103rd Cong. 32 (1993) (statement of Sen. John Kerry).

[4] Donald Rumsfeld, Op-Ed, *War of the Words*, Wall St. J., July 18, 2005, at A12.

[5] Info. Sec. Oversight Office, 2010 Report to the President 20 (2011) [hereinafter ISOO 2010 Report].

[6] Memorandum from O.G. Haywood, Jr., Colonel, Corps of Engineers, to Dr. [Harold] Fidler, Atomic Energy Commission, Medical Experiments on Humans (Apr. 17, 1947), *available at* http://www.hss.energy.gov/HealthSafety/ohre/roadmap/overview/074930/index.html.

[7] The National Security Archive has made the redacted and unredacted versions of the biographical sketch available at http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB90/index2.htm.

[8] William Burr, *Why Is "Poodle Blanket" Classified? Still More Dubious Secrets at the Pentagon*, Nat'l Sec. Archive (Apr. 7, 2010), http://www2.gwu.edu/~nsarchiv/nukevault/ebb310/index.htm.

[9] Exec. Order No. 13,526 § 1.1(b), 75 Fed. Reg. 707, 707 (Jan. 5, 2010).

[10] Comm'n on Protecting and Reducing Gov't Secrecy, Report of the Commission on Protecting and Reducing Government Secrecy, S. Doc. No. 105-2, at xxv (1997) [hereinafter Moynihan Commission Report].

[11] The President has ordered the heads of agencies to embark on a periodic "fundamental classification guidance review," with an eye toward "identify[ing] classified information that no longer requires protection and can be declassified." Exec. Order No. 13,526 § 1.9(a), 75 Fed. Reg. at 712. The first such review must be completed by June 29, 2012. *Id.* §§ 1.9(a), 6.3 at 712, 731. Unfortunately, early indicators suggest that some agencies have not approached this undertaking in a manner that is likely to produce meaningful change. *See* Steven Aftergood, *A Bumpy Start for Classification Review*, Secrecy News (Jan. 18, 2011), http://www.fas.org/blog/secrecy/2011/01/bumpy_fcgr.html.

[12] This proposal has long been advanced by experts and close observers of the classification system. *See, e.g.*, Moynihan Commission Report, *supra* note 10, at 37-38; Liberty and Sec. Comm., The Constitution Project, Reining in Excessive Secrecy: Recommendations for Reform of the Classification and Controlled Unclassified Information Systems 11 (2009), *available at* www.constitutionproject.org/pdf/178.pdf.

[13] *See, e.g.*, Mike German & Jay Stanley, Drastic Measures Required: Congress Needs to Overhaul U.S. Secrecy Laws and Increase Oversight of the Secret Security Establishment 48 (Am. Civ. Liberties Union 2011); *see also* Moynihan Commission Report, *supra* note 10, at 70 (recommending that the Director of Central Intelligence issue an Intelligence Community directive explaining the appropriate scope of the legislative protection for "sources and methods").

[14] Kevin R. Kosar, Cong. Research Serv., 97-771, Security Classification Policy and Procedure: E.O. 12958, as Amended 3 (2009).

[15] *See* Moynihan Commission Report, *supra* note 10, at app. G-1 (discussing Coolidge Committee).

[16] Def. Dep't Comm. on Classified Info., Report to the Secretary of Defense 6 (1956) [hereinafter Coolidge Committee Report].

[17] *See* Moynihan Commission Report, *supra* note 10, at app. G-1 (discussing Wright Commission).

[18] Comm'n on Gov't Sec., 84th Cong., Report of the Commission on Government Security 174-75 (1957).

[19] H.R. Rep. No. 85-1884, at 4 (1958) [hereinafter Moss Subcommittee Report].

[20] Def. Sci. Bd. Task Force on Secrecy, Report of the Defense Science Board Task Force on Secrecy 2 (1970).

[21] Comm'n to Review DOD Sec. Policies and Practices, Keeping the Nation's Secrets: A Report to the Secretary of Defense app. E, at 1 (1985).

[22] *Id.* at 31.

[23] Letter from Jeffery H. Smith to William J. Perry, Sec'y of Def., and R. James Woolsey, Dir. of Cent. Intelligence (Feb. 28, 1994), *reprinted in* Joint Sec. Comm'n, Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence ii (1994) [hereinafter Joint Security Commission Report].

[24] Joint Security Commission Report, *supra* note 23, at 6.

[25] Moynihan Commission Report, *supra* note 10, at xxi.

[26] Steven Aftergood, *Reducing Government Secrecy: Finding What Works*, 27 Yale L. & Pol'y Rev. 399, 404 (2009).

[27] 9/11 Commission Report, *supra* note 2, at 417.

[28] *See id.* at 353, 355, 417.

[29] *See* Moynihan Commission Report, *supra* note 10, at 36 (quoting McDaniel); *see also Emerging Threats: Overclassification and Pseudo-Classification: Hearing Before the Subcomm. on Nat'l Sec., Emerging Threats, and Int'l Relations of the H. Comm. on Gov't Reform*, 109th Cong. 115 (2005) [hereinafter *2005 Overclassification Hearing*] (written statement of Thomas Blanton, Exec. Dir., Nat'l Sec. Archive, George Wash. U.) (discussing McDaniel's statement).

[30] *Too Many Secrets: Overclassification as a Barrier to Critical Information Sharing: Hearing Before the Subcomm. on Nat'l Sec., Emerging Threats, and Int'l Relations of the H. Comm. on Gov't Reform*, 108th Cong. 82 (2004) (testimony of Carol A. Haave, Deputy Under Sec'y of Def., Counterintelligence and Sec.).

[31] *Intelligence Oversight and the Joint Inquiry: Hearing Before the Nat'l Comm'n on Terrorist Attacks Upon the U.S.* (testimony of Rep. Porter Goss), *available at* http://www.9-11commission.gov/archive/hearing2/9-11Commission_Hearing_2003-05-22.pdf.

[32] Moss Subcommittee Report, *supra* note 19, at 125.

[33] New York Times Co. v. United States, 403 U.S. 713 (1971).

[34] Erwin N. Griswold, Op-Ed, *Secrets Not Worth Keeping: The Courts and Classified Information*, Wash. Post, Feb. 15, 1989, at A25.

[35] Moynihan Commission Report, *supra* note 10, at 36.

[36] *See* Letter from Gregory L. Moulton, Exec. Sec'y, Agency Release Panel, Cent. Intelligence Agency, to Steven Aftergood, Senior Research Analyst, Fed'n of Am. Scientists (Dec. 14, 2000), *available at* http://www.fas.org/sgp/foia/1947/cia121400.pdf.

[37] Exec. Order No. 13,526 § 1.2(a)(3), 75 Fed. Reg. at 708.

[38] Confidential Cable from the U.S. Embassy Moscow on a Wedding in Dagestan (Aug. 31, 2006) (on file with the New York Times), *available at* http://www.nytimes.com/interactive/2010/11/28/world/20101128-cables-viewer.html#report/cables-06MOSCOW9533. The excerpted text is representative of the full paragraph.

[39] Exec. Order No. 13,526 § 1.2(a)(1), 75 Fed. Reg. at 707.

[40] Senate Select Comm. to Study Gov't Operations, Final Report of the Senate Select Committee to Study Government Operations: Intelligence Activities and the Rights of Americans, Book III, S. Rep. No. 94-755, at 125 (1976) [hereinafter Church Committee Final Report Book III].

[41] *Espionage in the Air Force Since World War II* (unpublished M.S. thesis, Defense Intelligence College), *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB90/dubious-06.pdf.

[42] For a discussion of privacy concerns raised by one information-sharing model (namely, fusion centers), *see* Michael German & Jay Stanley, What's Wrong With Fusion Centers? (2007), *available at* http://www.aclu.org/pdfs/privacy/fusioncenter_20071212.pdf.

[43] 9/11 Commission Report, *supra* note 2, at 355-56, 417.

[44] *Id.* at 417. As a member of 9/11 Commission would later testify, "The Commission found…that the failure to share information was the single most important reason why the U.S. Government failed to detect and disrupt the September 11 plot. There were bits and pieces of critical information available in different parts of the Government, in the CIA, the FBI, and the NSA….But pieces of the information were never shared and never put together in time to understand the September 11 plot." *2005 Overclassification Hearing*, *supra* note 29, at 88 (statement of Richard Ben-Veniste, Comm'r, Nat'l Comm'n on Terrorist Attacks Upon the U.S.).

[45] Homeland Sec. Advisory Council, Top Ten Challenges Facing the Next Secretary of Homeland Security 8 (2008).

[46] Michael T. Flynn et al., Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan 17 (2010), *available at* http://www.cnas.org/files/documents/publications/AfghanIntel_Flynn_Jan2010_code507_voices.pdf.

[47] *Id.* at 19.

[48] Janet Napolitano, Sec'y, U.S. Dep't of Homeland Sec., Lecture on Strength, Security, and Shared Responsibility: Preventing Terrorist Attacks a Decade After 9/11 (June 7, 2011), *available at* http://www.brennancenter.org/content/resource/strength_security_and_shared_responsibility_preventing_terrorist_attacks_a_.

[49] The Department of Homeland Security's description of fusion centers and their role may be found at *State and Major Urban Area Fusion Centers*, U.S. Dep't of Homeland Sec., http://www.dhs.gov/files/programs/gc_1156877184684.shtm (last visited Aug. 17, 2011).

[50] Official information about Joint Terrorism Task Forces may be found at *Joint Terrorism Task Force*, U.S. Dep't of Justice, http://www.justice.gov/jttf/ (last visited Aug. 17, 2011).

[51] *The Over-Classification and Pseudo-Classification: Part I, II, and III: Hearing Before the Subcomm. on Intelligence, Info. Sharing, and Terrorism Risk Assessment of the House Comm. on Homeland Sec.*, 110th Cong. 27 (2007) (statement of Chief Cathy L. Lanier, Metro. Police Dep't, Wash., D.C.) (emphasis omitted), *available at* http://www.fas.org/sgp/congress/2007/032207lanier.pdf. A colonel with the Illinois State Police similarly has testified:

> [E]ven when our fusion centers get information and our police chiefs get information, they can't pass it on to those commanders and patrol officers and detectives that need to use it because they don't have the ability, one, to declassify it; it can't be done rapidly; [tear] lines [i.e., the segregation of classified information to create an unclassified product] simply aren't working; and the system is designed to keep information secret, not to put it forward.

State and Local Fusion Centers and the Role of DHS: Hearing Before the Subcomm. on Emergency Preparedness, Sci., and Tech. of the H. Comm. on Homeland Sec., 109th Cong. 13 (2006) (testimony of Col. Kenneth Bouche, Ill. State Police).

[52] Coolidge Committee Report, *supra* note 16, at 6.

[53] *Id.* at 9.

[54] New York Times Co. v. United States, 403 U.S. 713, 730 (1971) (Stewart, J., concurring) ("For when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion. . . . [T]he hallmark of a truly effective internal security system would be the maximum possible disclosure, recognizing that secrecy can best be preserved only when credibility is truly maintained."); *see also* Moynihan Commission Report, *supra* note 10, at xxi ("The classification … system[] [is] no longer trusted by many inside and outside the Government….The best way to ensure that secrecy is respected, and that the most important secrets *remain* secret, is for secrecy to be returned to its limited but necessary role.").

[55] *2005 Overclassification Hearing*, *supra* note 29, at 64 (testimony of J. William Leonard, Dir., Info. Sec. Oversight Office).

[56] J. William Leonard, Dir., Info. Sec. Oversight Office, Remarks at the National Classification Management Society's Annual Training Seminar 4 (June 15, 2004), *available at* http://www.fas.org/sgp/isoo/leonard061504.pdf.

[57] U.S. Gov't Accountability Office, GAO-10-117T, Personnel Security Clearances 2 (2009), *available at* http://www.gao.gov/new.items/d10117t.pdf. The 2.4 million figure is in fact low because it "exclud[es] some of those with clearances who work in areas of national intelligence." *Id.* at 2.

[58] Richard Frost, *U.S. Says WikiLeaks Document Release Endangers Lives*, Businessweek (Nov. 28, 2010, 9:53 AM), http://www.businessweek.com/news/2010-11-28/u-s-says-wikileaks-document-release-endangers-lives.html.

[59] *Espionage Act and the Legal and Constitutional Issues Raised by WikiLeaks: Hearing Before the H. Comm. on the Judiciary*, 111th Cong. 86 (2010) (statement of Thomas S. Blanton, Dir., Nat'l Sec. Archive, George Wash. U.).

[60] *See, e.g.*, Diane Feinstein, Op-Ed, *Prosecute Assange Under the Espionage Act*, Wall St. J., Dec. 7, 2010, at A19; Eric W. Dolan, *Rep. Peter King Introduces Anti-WikiLeaks Legislation*, Raw Story (Feb. 15, 2011, 6:48 PM), http://www.rawstory.com/rs/2011/02/15/rep-peter-king-introduces-anti-wikileaks-legislation/ (discussing legislation introduced in the U.S. House of Representatives by Rep. Peter King (R-NY), along with similar legislation introduced in the U.S. Senate by Senators John Ensign (R-NV), Joe Lieberman (I-CT), and Scott Brown (R-MA), that would criminalize the publication of certain categories of classified information).

[61] Letter from James Madison to W.T. Barry (Aug. 4, 1822), *reprinted in* The Complete Madison 337 (Saul K. Padower ed., 1953).

[62] Haywood, *supra* note 6.

[63] *Id.*

[64] The executive branch argued that disclosing interrogation techniques would allow future detainees to practice resisting them. *See, e.g.*, Respondents' Memorandum in Opposition to Petitioners' Motion for Emergency Access to Counsel and Entry of Amended Protective Order 15-16, Khan v. Bush, No. 06-CV-1690 (D.D.C. Oct. 26, 2006), *available at* http://ccrjustice.org/ourcases/current-cases/khan-v.-obama-/-khan-v.-gates. But the United States waterboarded at least one detainee as many as 183 times, strongly suggesting that the policy's architects did not believe a detainee could become impervious to waterboarding through repeated exposure. *See* Scott Shane, *Waterboarding Used 266 Times on 2 Suspects*, N.Y. Times, April 20, 2009, at A1. Moreover, the Defense Department has long publicized the Army Field Manual that specifies permissible military interrogation techniques, and there is no indication that these techniques have been rendered ineffective through publication. *See Field Manual 2-22.3 Human Intel. Collector Operations*, Enlisted.info, http://www.enlisted.info/field-manuals/fm-2-22.3-human-intelligence-collector-operations.shtml (last visited July 1, 2011); *see also* John McCain, U.S. Senator (R-AZ), Floor Statement on Amendment on Army Field Manual (July 25, 2005), *available at* http://mccain.senate.gov/public/index.cfm?FuseAction=PressOffice.FloorStatements&ContentRecord_id=89b54ca0-574d-496b-8e88-d8edca2a92f8&Region_id=&Issue_id=1bd7f3a7-a52b-4ad0-a338-646c6a780d65 ("The Army Field Manual authorizes interrogation techniques that have proven effective in extracting life-saving information from the most hardened enemy prisoners.").

[65] Memorandum from John C. Yoo, Deputy Assistant Attorney Gen., to William J. Haynes II, Gen. Counsel of the Dep't of Def. 11-14, 39 (Mar. 14, 2003), *available at* http://www.fas.org/irp/agency/doj/olc-interrogation.pdf.

[66] *Secret Law and the Threat to Democratic and Accountable Government: Hearing Before the Subcomm. on the Constitution of the S. Comm. on the Judiciary*, 110th Cong. 11 (2008) (statement of J. William Leonard, Former Dir., Info. Sec. Oversight Office).

[67] Jack Goldsmith, The Terror Presidency 142-51, 166-67 (2007).

[68] Info. Sec. Oversight Office, 2010 Cost Report 1-2 (2011) [hereinafter ISOO 2010 Cost Report].

[69] *Id.* at 2.

[70] Joint Security Commission Report, *supra* note 23, at 94.

[71] Moynihan Commission Report, *supra* note 10, at 35.

[72] U.S. Gen. Accounting Office, GAO/NSIAD-94-55, Classified Information: Costs of Protection Are Integrated With Other Security Costs 15 (1993), *available at* http://archive.gao.gov/t2pbat4/150418.pdf.

[73] Kosar, *supra* note 14, at 3.

[74] Exec. Order No. 13,526, 75 Fed. Reg. 707 (Jan. 5, 2010); *see also* Memorandum: Implementation of the Executive Order, "Classified National Security Information," Dec. 29, 2009, 75 Fed. Reg. 733 (Jan. 5, 2010) [hereinafter Obama Implementing Memorandum], *available at* http://www.whitehouse.gov/the-press-office/presidential-memorandum-implementation-executive-order-classified-national-security.

[75] *See* Info. Sec. Oversight Office, 2006 Report to the President 24 (2007) [hereinafter ISOO 2006 Report].

[76] Exec. Order No. 13,526 § 1.3(a), (c), 75 Fed. Reg. at 708.

[77] Info. Sec. Oversight Office, Annual Report to the President: Fiscal Year 1979, at 3 (1980).

[78] ISOO 2010 Report, *supra* note 5, at 4-7.

[79] Exec. Order No. 13,526 § 1.1(a)(4), 75 Fed. Reg. at 707.

[80] *Id.* § 1.2(a)(1)-(3) at 707-08 (emphasis added).

[81] *Id.* § 1.4 at 709.

[82] *Id.* § 1.1(a)(4) at 707.

[83] *Id.* § 1.7(a)(1), (2) at 710.

[84] *Id.* § 1.7(b) at 710.

[85] *Cf.* Exec. Order No. 12,065 § 1-101, 43 Fed. Reg. 28,949, 28,950 (June 28, 1978) [hereinafter Carter Exec. Order], *with* Exec. Order No. 12,356 § 1.1(c), 47 Fed. Reg. 14,874, 14,874 (Apr. 2, 1982).

[86] Exec. Order No. 13,526 § 1.1(b), 75 Fed. Reg. at 707.

[87] *Id.* § 1.5(a) at 709.

[88] *Id.* § 1.5(b) at 709.

[89] *Id.* § 1.5(a) at 709.

[90] *Id.* § 1.5(d) at 709.

[91] ISOO 2010 Report, *supra* note 5, at 8.

[92] Exec. Order No. 13,526 § 1.5(a), 75 Fed. Reg. at 709.

[93] *Id.* § 1.6(a)(1) at 709.

[94] *Id.* § 1.6(c) at 710; *see also* Info. Sec. Oversight Office, Marking Classified National Security Information 5 (2010), *available at* http://www.archives.gov/isoo/training/marking-booklet.pdf.

[95] Exec. Order No. 13,526 § 1.6(a)(2), 75 Fed. Reg. at 709.

[96] *Id.* § 1.6(a)(3) at 709.

[97] *Id.* § 1.6(a)(4) at 709-10.

[98] *Id.* § 1.6(a)(5) at 710.

[99] *Id.* § 1.4(a) at 709.

[100] *Id.* § 1.6(g) at 710.

[101] *Id.*

[102] U.S. Gov't Accountability Office, *supra* note 57, at 1-2.

[103] Exec. Order No. 13,526 § 2.1(b)(3)(A), (B), 75 Fed. Reg. at 712.

[104] 32 C.F.R. § 2001.22(g) (2011).

[105] ISOO 2010 Report, *supra* note 5, at 24.

[106] Exec. Order No. 13,526 § 2.2(a), (b), 75 Fed. Reg. at 712-713.

[107] U. S. Dep't of State, Pub. No. DSCG-05-01, Classification Guide 16 (1st ed. 2005).

[108] ISOO 2010 Report, *supra* note 5, at 6, 8-9, 11.

[109] Exec. Order No. 13,526 § 2.1(b)(1), 75 Fed. Reg. at 712.

[110] *Id.* § 2.1(c) at 712.

[111] *Id.* § 2.1(d) at 712.

[112] *Id.* § 4.1(a) at 720.

[113] Exec. Order No. 12,968, 60 Fed. Reg. 40,245 (Aug. 7, 1995).

[114] *See* Office of Personnel Mgmt., Standard Form 86, Questionnaire for National Security Positions (2008), *available at* http://www.opm.gov/forms/pdf_fill/sf86.pdf.

[115] Exec. Order No. 12,968 § 3.1(b), 60 Fed. Reg. at 40,250.

[116] *See generally* Office of the Dir. of Nat'l Intelligence, Doc. No. 704.1, Intelligence Community Policy Guidance: Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information (2008), *available at* http://www.fas.org/irp/dni/icd/icpg704-1.pdf.

[117] *See* Info. Sec. Oversight Office, Standard Form 312, Classified Information Nondisclosure Agreement (2000), *available at* http://www.fas.org/sgp/isoo/new_sf312.pdf.

[118] *See id.*

[119] *See, e.g.*, U.S. Dep't of Def., Directive No. 5205.07, Special Access Program (SAP) Policy (2010), *available at* http://www.fas.org/irp/doddir/dod/d5205_07.pdf; Alice C. Maroni, Cong. Research Serv., IB 87201, Special Access Programs and the Defense Budget (1989), *available at* http://www.hsdl.org/?view&doc=74364&coll=limited; U.S. Dep't of the Army, Reg. No. 380-381, Special Access Programs (SAPs) and Sensitive Activities (2004), *available at* http://www.fas.org/irp/doddir/army/ar380-381.pdf.

[120] Exec. Order No. 13,526 § 1.5(a), 75 Fed. Reg. at 709.

[121] *Id.* § 3.3(a) at 714.

[122] *Id.* § 3.3(b)(6) at 714-15.

[123] *Id.* § 3.3 (h)(1) at 716-17.

[124] *Id.* §§ 3.3(h)(3), 5.3(a)(1) at 717, 724.

[125] Exec Order No. 12,958 § 3.4(a), 60 Fed. Reg. 19,825, 19,832-34 (Apr. 17, 1995).

[126] *Id.*

[127] *See* Pub. Interest Declassification Bd., Improving Declassification: A Report to the President 5 (2007) [hereinafter PIDB Report].

[128] Strom Thurmond National Defense Authorization Act for Fiscal Year 1999, Pub. L. No. 105-261, 112 Stat. 1920, § 3161(b)(1) (codified at 50 U.S.C. § 2672(b)(1) (2006)) (requiring review "on a page-by-page basis for Restricted Data and Formerly Restricted Data unless [particular records] have been determined to be highly unlikely to contain Restricted Data or Formerly Restricted Data"); 42 U.S.C. § 2014(y) (2006) (defining Restricted Data as "all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy"); *id.* § 2163 (defining the process by which Restricted Data becomes Formerly Restricted Data).

[129] Exec. Order No. 13,526 § 3.3(d)(3), 75 Fed. Reg. at 716; *see also Simplifying the Declassification Review Process for Historical Records*, Transforming Classification: Blog of the Public Interest Declassification Board (Mar. 29, 2011) [hereinafter *Simplifying Declassification Review*], http://blogs.archives.gov/transformingclassification/?p=110.

[130] PIDB Report, *supra* note 127, at 5-6.

[131] 44 U.S.C. § 2101-2120 (2006).

[132] David S. Ferriero, Archivist of the U.S., *Releasing All We Can, Protecting What We Must*, AOTUS Nat'l Archives (June 25, 2010), http://blogs.archives.gov/aotus/?p=1174.

[133] *See* Exec. Order No. 13,526 § 3.7(a), (b), 75 Fed. Reg. at 719-20; Obama Implementing Memorandum, *supra* note 74, at 733. Although reform of declassification policy is beyond the scope of this report, we note that many observers believe the backlog cannot be eliminated by the stated deadline without a fundamental change in policy, such as dispensing with review by all agencies that have "equities" in the classified document. *See, e.g.*, *Simplifying Declassification Review*, *supra* note 129.

[134] Exec. Order No. 13,526 § 3.5(a)(1), 75 Fed. Reg. at 718.

[135] *Id.* §§ 1.8(b)(3), 5.3(e)-(f), at 718, 725; 32 C.F.R. § 2001.14(b)(3) (2011).

[136] ISOO 2010 Report, *supra* note 5, at 1, 19-22, 25.

[137] 5 U.S.C. § 552(a)(4)(B), (a)(6)(A), (b)(1) (2006).

[138] *See, e.g.*, 28 C.F.R. § 16.7 (2011) ("[T]he originating component [within the Department of Justice] shall review the information to determine whether it should remain classified. Information determined to no longer require classification shall not be withheld."); 6 C.F.R. § 5.7 (2011) (similar Department of Homeland Security regulation).

[139] Aftergood, *supra* note 26, at 407.

[140] Exec. Order No. 13,526 § 1.8(b), 75 Fed. Reg. at 711.

[141] *Id.* § 1.8(b)(1), (3) at 711.

[142] ISOO 2010 Report, *supra* note 5, at 13.

[143] Carter Exec. Order, *supra* note 85, § 5-2 at 28,959.

[144] Exec. Order No. 13,526 § 5.2(b)(1), (b)(3), (b)(4), (b)(5), 75 Fed. Reg. at 723-24.

[145] ISOO 2010 Report, *supra* note 5, at 4-7, 11-12, 16-19.

[146] Info. Sec. Oversight Office, 2009 Report to the President 9, 18 (2010) [hereinafter ISOO 2009 Report]; Info. Sec. Oversight Office, 2008 Report to the President 23 (2009) [hereinafter ISOO 2008 Report]; Info. Sec. Oversight Office, 2007 Report to the President 25 (2008); ISOO 2006 Report, *supra* note 75 at 24; Info. Sec. Oversight Office, 2005 Report to the President 27 (2006) [hereinafter ISOO 2005 Report]; Info. Sec. Oversight Office, 2004 Report to the President 26 (2005).

[147] ISOO 2010 Report, *supra* note 5, at 23-24.

[148] Exec. Order No. 13,526 § 5.5(a), 75 Fed. Reg. at 726.

[149] *Id.* § 5.5(a), (b)(2) at 726.

[150] *Id.* § 5.5(c) at 726.

[151] *Id.* § 3.1(e) at 713.

[152] *Id.*

[153] E-mail from J. William Leonard, former Dir., Info. Sec. Oversight Office, to Elizabeth Goitein, Co-Dir., Liberty & Nat'l Sec. Program, Brennan Center for Justice (July 1, 2011, 3:39 p.m. EST) (on file with the Brennan Center); Telephone Interview with William J. Bosanko, former Dir., Info. Sec. Oversight Office (June 29, 2011).

[154] Exec. Order No. 13,526 § 5.3(a)(1)-(2), (b), 75 Fed. Reg. at 724, 725.

[155] Intelligence Authorization Act for Fiscal Year 2001, Pub. L. No. 106-567, § 703(a), 114 Stat. 2831, 2856 (2000) (amending 50 U.S.C.A. § 435 (West 2011)) (establishing the Public Interest Declassification Board).

[156] Memorandum for the Heads of Executive Departments and Agencies, Classified Information and Controlled Unclassified Information, 74 Fed. Reg. 26,277 (May 27, 2009); Martin Faga, *Declassification Policy Forum – Introduction*, The White House Open Gov't Initiative (June 29, 2009, 1:10 AM), http://www.whitehouse.gov/blog/Declassification-Policy-Forum-Introduction/.

[157] Obama Implementing Memorandum, *supra* note 74; Transforming Classification: Blog of the Public Interest Declassification Board, http://blogs.archives.gov/transformingclassification/.

[158] Moynihan Commission Report, *supra* note 10, at xliv.

[159] James B. Steinberg et al., Building Intelligence to Fight Terrorism**,** Brookings Institution Policy Brief, No. 125 1-2 (2003), *available at* http://www.brookings.edu/~/media/Files/rc/papers/2003/09intelligence_steinberg/pb125.pdf.

[160] *See, e.g.*, J. William Leonard, *The Corrupting Influence of Secrecy on National Policy Decisions*, *in* 19 Research in Social Problems and Public Policy: Government Secrecy 421, 423 (Susan Maret, ed., 2011) ("Official government secrecy is in many regards a relic of the Cold War that has long outlived its usefulness."). While commentators almost universally acknowledge the existence of a culture of secrecy, not all of them believe that the modern-day incarnation of this culture is a holdover from the Cold War. Former FBI official M.E. ("Spike") Bowman, for example, argues that the primary culprit is the string of executive orders governing classification and the procedures derived from those orders. *See* M.E. Bowman, *Dysfunctional Information Restrictions*, Fall/Winter 2006-2007 Intelligencer: Journal of U.S. Intelligence Studies 29, 29 (2007), *available at* http://www.fas.org/sgp/eprint/bowman.pdf ("[B]oth over-classification and over-long duration of classification are culturally governed by a decades-old process of protecting government information—a process that exudes an aura of reverence for the underlying theory behind them. . . ."). Bowman notes, however, that the "legacy instinct to classify information" that is enshrined in current classification procedures "did serve to protect the nation in a different era." *Id.* at 34.

[161] 9/11 Commission Report, *supra* note 2, at 417.

[162] Steinberg et al., *supra* note 159, at 2.

[163] *2005 Overclassification Hearing*, *supra* note 29, at 89 (statement of Richard Ben-Veniste, former Comm'r, Nat'l Comm'n on Terrorist Attacks Upon the U.S.).

[164] Francis Bacon, Religious Meditations, Of Heresies (1597), *reprinted in* The Works of Francis Bacon: Literary and Religious Works pt. III, 179 (New York, Hurd & Houghton 1873).

[165] Nathan Alexander Sales, *Secrecy and National Security Investigations*, 58 Ala. L. Rev. 811, 822 (2007).

[166] Aviam Soifer, *Born Classified, Born Free: An Essay for Henry Schwarzchild*, 19 Cardozo L. Rev. 1369, 1379-80 (1998).

[167] Ted Gup, Nation of Secrets: The Threat to Democracy and the American Way of Life 44 (2007); *see also* Robert D. Steele, Open Source Intelligence: What is It? Why is it Important to the Military? 337 (1997), *available at* http://www.oss.net/dynamaster/file_archive/040320/fb893cded51d5ff6145f06c39a3d5094/OSS1997-02-33.pdf ("Culturally there is a strong attitude, primarily within the intelligence community but to an extent within the operational community, that information achieves a special value only if it is classified. This is in part a result of a cultural inclination to treat knowledge as power, and to withhold knowledge from others as a means of protecting one's power.").

[168] Gup, *supra* note 167, at 46 (quoting Harold Relyea, longtime secrecy expert formerly with the Congressional Research Service).

[169] Max Weber, Bureaucracy, *reprinted in* From Max Weber: Essays in Sociology 196, 233-34 (H.H. Gerth & C. Wright Mills eds., trans., 1946).

[170] Dana Priest & William M. Arkin, *Top Secret America: A Hidden World, Growing Beyond Control*, Wash. Post, July 19, 2010, at A1.

[171] *See* Sales, *supra* note 165, at 822 ("Secrecy . . . can precipitate a form of informational turf war. This danger is especially acute in the national security context, in which various agencies (such as the FBI, CIA, and NSA) have overlapping responsibilities and thus have reason to regard one another as competitors.") (internal footnote and citation omitted).

[172] C3I: Issues of Command and Control 68 (Thomas P. Croakley ed., 1991) (*quoting* Rodney McDaniel, former Exec. Sec'y of the Nat'l Sec. Council).

[173] Daniel Patrick Moynihan, Secrecy: The American Experience 73 (1998).

[174] *See* Homeland Security Advisory Council, *supra* note 45, at 8 (noting that the "need to know" requirement can serve as a "barrier (and often an excuse) for not sharing pertinent information with homeland security partners"); *see also* Bowman, *supra* note 160, at 32 (noting the "possessory instincts of agency employees who have worked hard to accumulate information").

[175] Priest & Arkin, *supra* note 170, at A1. Of course, the failure to share information among agencies is not entirely attributable to inter-agency competition. Much of the problem stems from more mundane administrative issues such as the maintenance of separate classified computer systems that are not sufficiently interoperable. *See id.* at A1 (noting that "[t]he data flow [at the National Counterterrorism Center] is enormous, with dozens of databases feeding separate computer networks that cannot interact with one another. There is a long explanation for why these databases are still not connected, and it amounts to this: It's too hard, and some agency heads don't really want to give up the systems they have"). The culture of secrecy is nonetheless indirectly responsible for such obstacles, as they presumably would have been overcome—or perhaps not have emerged in the first place—if agencies harbored different attitudes toward the relative value of secrecy and openness.

[176] *See generally* James L. Gibson et al., Organizations: Behavior, Structure, and Processes (1994).

[177] Exec. Order No. 13,526 § 1.7(a)(1)-(2), 75 Fed. Reg. at 710.

[178] *See* ACLU v. Dep't of Defense, 628 F.3d 612 (D.C. Cir. 2011) (interpreting the prohibition on using classification to conceal misconduct).

[179] Haywood, *supra* note 6.

[180] *See* Aftergood, *supra* note 26, at 403.

[181] Moss Subcommittee Report, *supra* note 19, at 4 (1958).

[182] *Id.*

[183] *See* Charlie Savage & James Risen, *Federal Judge Finds N.S.A. Wiretaps Were Illegal*, N.Y. Times, Mar. 31, 2010, at A1.

[184] Memorandum from the U.S. Dep't of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President (Jan. 19, 2006), *available at* http://www.justice.gov/opa/whitepaperonnsalegalauthorities.pdf.

[185] *See* Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (codified in scattered sections of 50 U.S.C.); Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2435 (codified in scattered sections of 50 U.S.C. and 18 U.S.C.); Joby Warrick & Walter Pincus, *How the Fight for Vast New Spying Powers Was Won*, Wash. Post, Aug. 12, 2007, at A1.

[186] Erwin N. Griswold, Op-Ed, *Secrets Not Worth Keeping: The Courts and Classified Information*, Wash. Post, Feb. 15, 1989, at A25.

[187] *Mark-up of Fiscal Year 1994 Foreign Relations Authorization Act: Hearing Before the Subcomm. on Terrorism, Narcotics, and Int'l Operations of the S. Comm. on Foreign Relations*, 103rd Cong. 32 (1993) (statement of Sen. John Kerry).

[188] *See, e.g.*, The Federalist No. 70, at 78 (Alexander Hamilton) (Clinton Rossiter ed., 1961); The Federalist No. 64, at 393 (John Jay) (Clinton Rossiter ed., 1961); John Adams, Thoughts on Government (1776), *reprinted in* The Works of John Adams 193, 196 (Boston, Charles C. Little & James Brown 1851); The Papers of George Mason 896-98 (Robert Rutland ed., 1970).

[189] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of U.S.C.); Authorization for Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001).

[190] The Federalist No. 70, at 424 (Alexander Hamilton) (Clinton Rossiter, ed.,1961).

[191] Gup, *supra* note 167, at 28-29 (quoting former covert CIA operative Melissa Mahle).

[192] Church Committee Final Report Book III, *supra* note 40, at 125.

[193] *See* Jeffrey Richelson et al., eds., *Dubious Secrets*, Nat'l Sec. Archive Electronic Briefing Book No. 90 (May 21, 2003), http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB90/index.htm.

[194] Manu Raju et al., *Few Senators Read Iraq NIE Report*, The Hill (June 19, 2007), http://thehill.com/homenews/news/12304-few-senators-readiraqniereport.

[195] Select Comm. on Intelligence, Report of the Select Committee on Intelligence on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq, S. Rep. No. 108-301, at 295 (2004), *available at* http://intelligence.senate.gov/108301.pdf. Classification and excessive compartmentation even prevented some executive officials from learning key information: the Defense Intelligence Agency concluded that one key Iraqi source of information about WMDs was a "fabricator" and attached a warning notice to his report, "but the notice was so highly restricted that other intelligence officials never saw it." Evan Thomas et al., *The Rise and Fall of Chalabi: Bush's Mr. Wrong*, Newsweek, May 31, 2004, at 22.

[196] Authorization for Use of Military Force Against Iraq Resolution of 2002, Pub. L. No. 107-243, 116 Stat. 1498 (2002).

[197] *See* Katharine Q. Seelye, *Threats and Responses: The Detainees*, N.Y. Times, Oct. 23, 2002, at A14; Joby Warrick, *A Blind Eye to Guantánamo?*, Wash. Post, July 12, 2008, at A2; Donald Rumsfeld, Sec'y of Def., DoD News Briefing with Secretary Rumsfeld and General Pace (June 14, 2005), *available at* http://www.defense.gov/Transcripts/Transcript.aspx?TranscriptID=3854.

[198] BBC, *WikiLeaks: Many at Guantanamo 'Not Dangerous,'* BBC News (Apr. 25, 2011), http://www.bbc.co.uk/news/world-us-canada-13184845.

[199] Coolidge Committee Report, *supra* note 16, at 3.

[200] Moss Subcommittee Report, *supra* note 19, at 158; *see also* Bowman, *supra* note 160, at 34 (noting that, in contrast to the absence of sanctions for overclassification, "revealing 'too much' generally has been considered career-threatening").

[201] 9/11 Commission Report, *supra* note 2, at 417.

[202] J. William Leonard, Dir., Info. Sec. Oversight Office, at the National Classification Management Society Annual Training Seminar (June 12, 2003); *see also* Geoffrey R. Stone, *Government Secrecy v. Freedom of the Press*, 1 Harv. L. & Pol'y Rev. 185, 192-93 (2007) ("[T]he classification process is poorly designed and sloppily implemented. Predictably, the government tends to *over*-classify information. An employee charged with the task of classifying information inevitably will err on the side of over-classification because no employee wants to be responsible for *under*-classification.").

[203] *See, e.g.*, Jonah Goldberg, Op-Ed, *Fort Hood Killings: FBI Asleep on the Job*, Sun Sentinel (Ft. Lauderdale), Nov. 17, 2009, at A21; Scott Shane & David Johnston, *Republicans Seek Inquiry on Fort Hood*, N.Y. Times, Nov. 18, 2009, at A22; Tim Rutten, Op-Ed, *What Did, and Didn't, the Army Know?*, L.A. Times, Nov. 11, 2009, at 23.

[204] Exec. Order No. 13,526 § 1.4, 75 Fed. Reg. at 709.

[205] *Id.* § 1.2 at 707-708.

[206] *See supra* Chapter 3 Part A.4 & *infra* Chapter 3 Part B.2.

[207] Project on Nat'l Sec. Reform, Forging a New Shield 304 (2008), *available at* http://pnsr.org/data/files/pnsr%20forging%20a%20new%20shield.pdf; *see also* National Defense Authorization Act for Fiscal Year 2008, Pub. L. No. 110-181, § 1049, 122 Stat. 3, 317 (2008) (directing the Department of Defense to contract with an independent organization to study national security reform). The observations in this section are also based on interviews with current and former government officials who asked not to be identified (notes of interviews on file with the Brennan Center).

[208] Exec. Order No. 13,526 § 1.1(a)(4), 75 Fed. Reg. at 707 (emphasis added).

[209] 32 C.F.R. § 2001.10 (2011) ("There is no requirement, at the time of the decision, for the original classification authority to prepare a written description of such damage. However, the original classification authority must be able to support the decision in writing, including identifying or describing the damage, should the classification decision become the subject of a challenge or access demand.").

[210] Exec. Order No. 12,958 § 1.7(a)(5), 60 Fed. Reg. at 19,828.

[211] Moynihan Commission Report, *supra* note 10, at 30.

[212] Exec. Order No. 13,526 § 6.1(s), 75 Fed. Reg. at 728.

[213] 32 C.F.R. § 2001.22(c)(1).

[214] The default setting can be "Unclassified," a practice followed in at least one agency, according to interviews with current and former government officials (notes of interviews on file with the Brennan Center). This fact underscores the point that, while technology can exacerbate overclassification, it can help reduce it, as well. *See* Chapter 4 Part A, *infra* (proposing use of electronic forms to promote careful deliberation).

[215] Little public information is available regarding the features of the many different automated systems used by agencies and components engaged in classification activity. The description in this report is based on multiple interviews with current and former government employees who routinely work or worked with classified computer systems (notes of interviews on file with the Brennan Center).

[216] 32 C.F.R. §§ 2001.21(a)(1), 2001.22(b), (c).

[217] Under the previous executive order, the list need only be appended to the official file or record copy of the classified document. *See* Exec. Order No. 12,958 § 2.1(b)(2)(B), 68 Fed. Reg. 15,315, 15,319 (Mar. 25, 2003) (as amended by Exec. Order No. 13,292, 68 Fed. Reg. 15,315 (Mar. 25, 2003)). Under the current executive order and implementing directive, the list must be on or attached to each derivatively classified document. *See* Exec. Order No. 13,526 § 2.1(b)(3)(B), 75 Fed. Reg. at 712; 32 C.F.R. § 2001.22(c)(1)(ii).

[218] ISOO 2009 Report, *supra* note 146, at 18.

[219] ISOO 2006 Report, *supra* note 75, at 24.

[220] ISOO 2009 Report, *supra* note 146, at 18.

[221] *See* Memorandum from Jay S. Bybee, Assistant Attorney Gen., to John Rizzo, Acting Gen. Counsel of the Cent. Intelligence Agency, Interrogation of Al Qaeda Operative (Aug. 1, 2002), *available at* http://www.fas.org/irp/agency/doj/olc/zubaydah.pdf.

[222] 9/11 Commission Report, *supra* note 2, at 417.

[223] *See* Moss Subcommittee Report, *supra* note 19, at 158; Coolidge Committee Report, *supra* note 16, at 3.

[224] Bowman, *supra* note 160, at 34.

[225] Exec. Order No. 11,652 § 13(A), 37 Fed. Reg. 5209, 5218 (Mar. 8, 1972).

[226] Carter Exec. Order, *supra* note 85, § 5-502(a) & 503, at 28,961.

[227] Exec. Order No. 13,526 § 5.5(b), (b)(2), 75 Fed. Reg. at 726 (requiring sanctions for those who "knowingly, willfully, or negligently" "classify or continue the classification of information in violation of this order or any implementing directive").

[228] Comm'n to Review DOD Sec. Policies, *supra* note 21, at 31.

[229] Joint Security Commission Report, *supra* note 23, at 25.

[230] Exec. Order No. 13,526 § 5.4(d)(4), 75 Fed. Reg. at 725-26.

[231] ISOO 2005 Report, *supra* note 146, at 26.

[232] Exec. Order No. 12,958 § 5.4(d)(7), 68 Fed. Reg. at 15,329 (as amended by Exec. Order No. 13,292); ISOO 2008 Report, *supra* note 146, at 22.

[233] Leading experts in classification were unaware of such an instance. E-mail from J. William Leonard, former Dir., Info. Sec. Oversight Office, to Elizabeth Goitein, Co-Dir., Liberty & Nat'l Sec. Program, Brennan Center for Justice (July 1, 2011, 3:39 p.m. EST) (on file with the Brennan Center); e-mail from Steven Aftergood, Dir., Project on Gov't Secrecy, Fed'n of Am. Scientists, to David M. Shapiro, Counsel, Brennan Center for Justice (June 22, 2010, 1:03 p.m. EST) (on file with the Brennan Center).

[234] Exec. Order No. 13,526 § 4.1(b), 75 Fed. Reg. at 720.

[235] Exec. Order No. 12,958 § 1.3(d), 68 Fed. Reg. at 15,316 (as amended by Exec. Order No. 13,292).

[236] 32 C.F.R. § 2001.70(a), 2001.71(a) (2009) (amended 2010).

[237] *See, e.g.*, ISOO 2008 Report, *supra* note 146, at 23; ISOO 2006 Report, *supra* note 75, at 23; ISOO 2005 Report, *supra* note 146, at 26; *see also* 32 C.F.R. § 2001.70(e) (2009) (amended 2010) (setting forth requirement of annual refresher training).

[238] ISOO 2008 Report, *supra* note 146, at 23.

[239] Information about the nature of classification trainings was provided/confirmed by current and former government employees who participated in such trainings and who asked not to be identified (notes of interviews on file with the Brennan Center).

[240] *See, e.g.*, ISOO 2008 Report, *supra* note 146, at 23 ("[T]he high percentage of documents with errors . . . suggests many agencies' classified national security information programs would benefit from additional training on the classification and marking of documents.").

[241] Telephone Interview with J. William Leonard, former Dir., Info. Sec. Oversight Office (Apr. 15, 2011).

[242] Exec. Order No. 13,526 § 1.8(a), 75 Fed. Reg. at 711.

[243] *Id.* § 1.8(b) at 711.

[244] ISOO 2010 Report, *supra* note 5, at 13. While ISOO's implementing directive notes that authorized holders should be encouraged to question classification decisions outside the formal challenge system, *see* 32 C.F.R. § 2001.14(c)(2) (2011), ISOO does not report statistics on how often such informal challenges occur.

[245] *See supra* Chapter 1 Part A.

[246] ISOO 2010 Report, *supra* note 5, at 13.

[247] ISOO 2009 Report, *supra* note 146, at 19; ISOO 2008 Report, *supra* note 146, at 22-23.

[248] 32 C.F.R. § 2001.14(a).

[249] Moynihan Commission Report, *supra* note 10, at xxv.

[250] *Id*. at xxv-xxvi.

[251] The case for pilot projects has been persuasively advanced by classification expert Steven Aftergood. *See* Aftergood, *supra* note 26, at 412-13.

[252] *See* U.S. Gen. Accounting Office, *supra* note 72, at 15.

[253] Exec. Order No. 13,526 § 1.1(a)(4), 75 Fed. Reg. at 707.

[254] *See Reconsidering Information Management in the Electronic Environment*, Transforming Classification: Blog of the Public Interest Declassification Board (Mar. 14, 2011), http://blogs.archives.gov/transformingclassification/?p=55.

[255] Moynihan Commission Report, *supra* note 10, at 30-31.

[256] Exec. Order No. 13,526 § 1.6(a)(1)-(3), 75 Fed. Reg. at 709-710; 32 C.F.R. § 2001.21(a)(1), (a)(2), (b), (e).

[257] Exec. Order No. 13,526 § 1.2(a), 75 Fed. Reg. at 707-08.

[258] *Id.* § 1.1(a)(4) at 707.

[259] *Id.* § 1.4 at 709.

[260] *Id.* § 1.7(a)(1)-(4) at 710.

[261] *Id.* § 1.6(g) at 710. The remaining portions of Question 7 reflect the following requirements contained in the executive order: (1) "[i]f there is significant doubt about the appropriate level of classification, [a document] shall be classified at the lower level," *id.* § 1.2(c) at 708; (2) "[b]asic scientific information not clearly related to the national security shall not be classified," *id.* §1.7(b) at 710; and (3) absent a waiver of the portion marking requirement from ISOO, "the agency originating the document shall, by marking or other means, indicate which portions are classified, with the applicable classification level, and which portions are unclassified," *id.* § 1.6(c) at 710.

Classification in certain circumstances requires compliance with additional requirements. Examples include classification of previously unclassified information after an individual makes a request for the information under laws such as FOIA, *id.* § 1.7(d) at 711, and reclassification of previously declassified documents, *id.* § 1.7(c) at 710-11. Variations on the form used in such circumstances should include the additional requirements that apply.

[262] *Id.* § 1.5(a) at 709.

[263] *Id.* § 1.5(b) at 709.

[264] *Id.* § 1.5(a) at 709.

[265] *See supra* note 11. The importance of revising agency classification guides to include only specific, readily-identifiable categories of information cannot be overstated. It is not included as a recommendation in this report because the report focuses on a different aspect of the overclassification problem, namely, how to ensure compliance with the criteria for classification. *See* text accompanying note 11.

[266] *See* Telephone Interview with J. William Leonard, *supra* note 241 and accompanying text.

[267] 32 C.F.R. § 2001.22 (c)(1) (2011).

[268] *See, e.g.*, U. S. Dep't of State, *supra* note 107, at 6 (noting that "[o]ften there are multiple considerations in determining the duration of classification" and stating that "[i]t is . . . incumbent upon the user of this guide . . . carefully to consider each duration decision").

[269] Exec. Order No. 13,526 § 2.1(c); 32 C.F.R. § 2001.22(g).

[270] Exec. Order No. 13,526 § 2.1(b)(3)(B), 75 Fed. Reg. at 712; 32 C.F.R. § 2001.22(c)(1).

[271] Exec. Order No. 13,526 § 2.1(b)(3)(B), 75 Fed. Reg. at 712; 32 C.F.R. § 2001.22(c)(1)(ii).

[272] Exec. Order No. 13,526 § 1.1(b), 75 Fed. Reg. at 707.

[273] *Id.* § 2.1(b)(1) at 712.

[274] The current executive order requires agencies to include "designation and management of classified information" as a critical element in the personnel performance ratings of those who regularly deal with classified information. *Id.* § 5.4(d)(7) at 726. In theory, this requirement provides a mechanism for accountability. However, as noted in Chapter 3, the previous executive order required agencies to rate employees on "management of classified information," Exec. Order No. 12,958 § 5.4(d)(7), 68 Fed. Reg. at 15,329 (as amended by Exec. Order No. 13,292), and even this narrower requirement was frequently ignored by agencies. *See* ISOO 2008 Report, *supra* note 146, at 22 (noting that four out of six agencies visited by ISOO in fiscal year 2008 did not comply with this requirement); *see also supra* note 232 and accompanying text. Audits by agencies' Offices of the Inspector General, as proposed in this report, are more likely to be effective because they do not rely on busy supervisors to conduct in-depth assessments of employees' classification decisions.

[275] Inspector General Act of 1978, 5 U.S.C. app. §§ 3(a)-(b), 8G (2006).

[276] In designating one or two agencies to serve as test agencies for the proposed pilot project, the President should specify that the self-inspection programs at those agencies need not include "regular reviews of representative samples of the agency's original and derivative classification actions," Exec. Order No. 13,526 § 5.4(d)(4), 75 Fed. Reg. at 725, as this function largely will be served by the OIG audits.

[277] *See, e.g.*, ISOO 2006 Report, *supra* note 75, at 23; ISOO 2005 Report, *supra* note 146, at 26. The same problem—i.e., lack of support from senior agency management—would likely undermine the 1994 proposal by the Joint Security Commission that each agency appoint an ombudsman to review samples of the agency's classified product and identify individuals responsible for classification errors. *See* Joint Security Commission Report, *supra* note 23, at 25.

[278] 50 U.S.C.A. § 435 note (West 2009) (Promotion of Accurate Classification of Information).

[279] Inspector General Act of 1978, 5 U.S.C. app. § 6.

[280] Frederick M. Kaiser, Cong. Research Serv., 98-379, Statutory Offices of Inspector General 2 (2008).

[281] *See, e.g.*, Inspector General Act of 1978, 5 U.S.C. app. § 8I(a)(1) (2006) (granting the Secretary of Homeland Security "authority, direction, and control" of Inspector General "audits or investigations, or the issuance of subpoenas, that require access to sensitive information concerning" matters such as intelligence, counterintelligence, or counterterrorism matters); *id.* at § 8(b) (similar provisions regarding Department of Defense). Due to these restrictions, the agencies in question should not be selected as test agencies for the pilot project.

[282] *See, e.g.*, ISOO 2009 Report, *supra* note 146, at 18.

[283] The President could amend his executive order to include this role among those currently specified. *See* Exec. Order No. 13,526 § 5.3(b), 75 Fed. Reg. at 724.

[284] In 1999, the Chair of ISCAP noted in public remarks that nearly 85 percent of the Panel's decisions were unanimous. *See* Roslyn A. Mazer, Chair, Interagency Sec. Classification Appeals Panel, Remarks on Security Classification Appeals (Apr. 1, 1999), *available at* http://www.firstamendmentcenter.com/news.aspx?id=5629.

[285] Edgar H. Schein, *Organizational Culture*, 45 Am. Psychologist 109, 111 (1990); *see also* David A. Nadler & Michael L. Tushman, *Beyond the Charismatic Leader: Leadership and Organizational Change*, 32 Cal. Mgmt. Rev. 77, 77 (1990).

[286] Exec. Order No. 13,526 § 5.4(a), (b), 75 Fed. Reg. at 725.

[287] Moynihan Commission Report, *supra* note 10, at 39; *see also* J. William Leonard, Dir., Info. Sec. Oversight Office, Remarks at the National Classification Management Society Annual Training Seminar 2 (June 15, 2004) ("[T]he security classification system works, and its integrity is preserved, only when agency leadership demonstrates personal commitment and commits senior management to make it work.").

[288] *See* Aftergood, *supra* note 26, at 413-14.

[289] There is one important caveat to this observation. Senators Kyl and Lott claimed that Secretary O'Leary's initiative had resulted in the release of nuclear secrets, and on that basis introduced the so-called "Kyl-Lott amendment," discussed at Chapter 2, Part D.1, *supra*. *See* Steven Aftergood, *Openness and Secrecy at the Department of Energy After the China Espionage Investigations*, 53 J. of the Fed'n of Am. Scientists (2000), http://www.fas.org/faspir/v53n1a.htm.

[290] Aftergood, *supra* note 26, at 409-10.

[291] Exec. Order No. 13,526 §§ 1.3(d), 2.1(d), 75 Fed. Reg. at 708, 712.

[292] *See supra* Chapter 3 Part B.3.

[293] *See, e.g.*, ISOO 2007 Report, *supra* note 146, at 23 ("Insufficient security staff is a direct cause of the failure of some agencies to implement essential program elements, such as security education and training . . . .").

[294] ISOO 2010 Cost Report, *supra* note 68, at 3.

[295] *See* ISOO 2009 Report *supra* note 146, at 19 (noting that "additional training requirements for all original and derivative classifiers . . . should lead to greater accuracy and reduce over-classification").

[296] *See* Exec. Order No. 13,526 § 5.2(b)(3), 75 Fed. Reg. at 723-24.

[297] Public meeting of the Public Interest Declassification Board, May 26, 2011 (notes of meeting on file with the Brennan Center). Minutes of the meeting were not available at time of writing, but Board meeting minutes generally are available at http://www.archives.gov/pidb/meetings/.

[298] Exec. Order No. 13,526 § 1.1(a), 75 Fed. Reg. at 707 (emphasis added).

[299] *See* Leonard, *supra* note 160, at 428 (noting that "the failure to balance the damage that results from disclosure, with the damage that results from classifying, can have exceedingly tragic consequences for our nation").

[300] *Discretionary Declassification and Release of Contemporary National Security Information*, Transforming Classification: Blog of the Public Interest Declassification Board (Mar. 29, 2011), http://blogs.archives.gov/transformingclassification/?p=116.

[301] Exec. Order No. 13,526 § 2.1(b)(2), 75 Fed. Reg. at 712.

[302] This specification is necessary because, in the different but analogous case of whistleblowers, "[t]aking away an employee's security clearance has become the weapon of choice for wrongdoers who retaliate." Project on Gov't Oversight, Homeland and National Security Whistleblower Protections: The Unfinished Agenda 26 (2005), *available* at http://www.pogoarchives.org/m/gp/wbr2005/WBR-04282005.pdf. Yet, in a memorandum discussing the Whistleblower Protection Act, the Justice Department's Office of Legal Counsel opined that the revocation of a security clearance does not qualify as a "personnel action" and therefore was not a prohibited retaliatory action under the Act. *See* Louis Fisher, Cong. Research Service, RL 33215, National Security Whistleblowers 31 (2005).

[303] Exec. Order No. 13,526 § 1.8(a), 75 Fed. Reg. at 711.

[304] An idea along these lines was proposed by Mike German, Policy Counsel for the American Civil Liberties Union, at a July 8, 2009 public meeting of the Public Interest Declassification Board. *See* Pub. Interest Declassification Bd., Minutes of the Meeting 2 (July 8, 2009), *available at* http://www.archives.gov/pidb/meetings/07-08-09.pdf.

[305] 5 U.S.C. §§ 4503, 4504 (2006).

[306] 50 U.S.C.A. § 435 note (West 2009) (Promotion of Accurate Classification of Information).

[307] Moss Subcommittee Report, *supra* note 19, at 4.

[308] Homeland Security Advisory Council, *supra* note 45, at 8.

[309] Memorandum of January 21, 2009: Freedom of Information Act, 74 Fed. Reg. 4,683 (Jan. 26, 2009), *available at* http://www.neh.gov/whoweare/foia/FOIA_Presidents-Memorandum.pdf.

NEW & FORTHCOMING BRENNAN CENTER PUBLICATIONS

Rethinking Radicalization
Faiza Patel

Domestic Intelligence: New Powers, New Risks
Emily Berman

Money, Politics, and the Constitution: Beyond Citizens United
Edited by Monica Youn

A Report Card on New York's Civic Literacy
Eric Lane and Meg Barnette

A Media Guide to Redistricting
Erika Wood and Myrna Pérez

Transparent Elections after Citizens United
Ciara Torres-Spelliscy

Meaningful Ethics Reform for the "New" Albany
Lawrence Norden, Kelly Williams, and John Travis

Criminal Justice Debt: A Barrier to Reentry
Alicia Bannon, Mitali Nagrecha, and Rebekah Diller

Small Donor Public Funding: The NYC Experience
Susan Liss and Angela Migally

Voting System Failures: A Database Solution
Lawrence Norden

New Politics of Judicial Elections 2000-2009
James Sample, Adam Skaggs, and Jonathan Blitzer

For more information, please visit www.brennancenter.org

BRENNAN
CENTER
FOR JUSTICE

at New York University School of Law

161 Avenue of the Americas
12th Floor
New York, NY 10013
www.brennancenter.org