Perspective
EXPERT INSIGHTS ON A TIMELY POLICY ISSUE

November 2018

JAMES B. BRUCE, SINA BEAGHLEY, W. GEORGE JAMESON

Secrecy in U.S. National Security

Why a Paradigm Shift Is Needed

Contents

Cover photos, clockwise from top left: Todd Taulman/Adobe Stock; Halfdark/Getty Images; Lars Plougmann/Flickr; evgeniya_m/Adobe Stock; Dori Gordon Walker.

For more information on this publication, visit www.rand.org/t/PE305.

This Perspective summarizes our key findings and conclusions regarding the adequacy of the present system governing secrecy in U.S. national security information. This work, based on a novel approach and expert opinion—including our own direct experience with the issues—aims to provide recommendations to improve the system that makes, safeguards, and discloses secrets. An improved system will afford significantly better protection to secrets that truly need it, reduce overclassification by providing clear parameters for creating secrets, and more fully support government transparency goals.

The impetus for this examination of secrecy issues came from two related but seemingly contradictory considerations. On one hand, there are significant high-level concerns about damage to national security through the public availability of massive amounts of classified information on the internet, as exemplified by the unprecedented scale of unauthorized disclosures by Edward Snowden and Private Bradley (now Chelsea) Manning on WikiLeaks and in news media accounts.[1] On the other hand, advocates of greater transparency in government continue to voice concerns that national interests are harmed because the government keeps too much information classified about its operations and their impact on the public.[2] Both these critiques suggest that the current secrecy system is failing to fulfill its principal purposes: first, protecting classified information critical to national security and, second, reducing overclassification and officially disclosing classified information to further government transparency and accountability.

To test our premise that the secrecy system is generally failing to meet these key goals and thus needs repair, we conducted an extensive literature review; interviewed current and former senior U.S. government officials and other subject-matter experts (SMEs) and stakeholders; and benefited from insightful commentary from a one-day workshop, "Assessing the Secrecy Paradigm for the Future Information Environment," which was convened in partnership with the American Bar Association's Standing Committee on Law and National Security. Informed by these data, we analyzed key factors that drive how well or how poorly the system for national security secrecy works—and why. (For elaboration, see the appendix.)

What Is a Secret?

We define a "secret" as any national security information that has been officially classified by the U.S. government as Confidential, Secret, or Top Secret.

Adapting Thomas Kuhn's use of "paradigm" for its conceptual framework, we examined the principal elements (the structure, culture, rules, and technologies of conducting secrecy) of the secrecy paradigm and its processes (the classification of information, how it is safeguarded, and how it becomes available to the public). Together, the way these elements and processes perform individually and interact with each other determines the overall performance of the secrecy paradigm. We evaluated this performance and, where it is found wanting, offer recommendations to improve it. Notably, we identified no arguments, even from current government security practitioners who might be expected to resist reform, in favor of retaining the status quo. At the same time, we found no compelling suggestions for any alternative approach that could replace the current secrecy paradigm. Accordingly, we offer observations and recommendations for what we call a "paradigm shift" that we believe would, if implemented, substantially improve the way official secrets are created, protected, and released.

The Secrecy Paradigm

When we describe secrecy as a paradigm, following Kuhn's emphasis on problem-solving ideas and the professionals engaged in them,[3] we refer to both the essential body of ideas about secrecy and the national security practitioners that produce and implement these ideas. In the contemporary United States, keeping secrets safe to help protect the security of the nation and the countervailing aims to limit the creation of secrets in the name of openness and transparency—both key principles of Executive Order (EO) 13526[4]—are the twin problems that the present secrecy paradigm is supposed to solve. The headline challenges that the present secrecy paradigm faces are largely a result of the failure of adaptation. The present secrecy paradigm was created in the years after World War II, when secrets, and the people cleared for access to them, were far fewer. Secrets were produced only in hard copy and protected in safes, without electronic means of proliferation. As technology advanced and secrets proliferated—both at transformative rates—secrecy protection did not keep pace, and neither did a much-hoped-for improvement in transparency. For many inside the system, and for others critiquing it from the outside, the performance of the present secrecy paradigm is simply failing to adapt to the Information Age. If a failing paradigm cannot solve its legacy problems, it should be modernized or replaced by one that will. Even without a complete replacement, the old system can still undergo a paradigm shift that will come closer to full success in solving the 21st-century problems of managing secrecy. Our selection of paradigm as a conceptual model to examine secrecy is motivated partly by the inherent power of the concept (below) and by the shortcomings of the present literature examining the subject.

In general, the voluminous literature on secrecy can be sorted into three loosely defined genres:

- "big picture" advocacy arguments that secrecy is excessive and reducing it should be a top priority,[5]

or that secrecy is so vital to national security that reducing it should be only a secondary goal[6]
- narrow-focus studies of technical or other secrecy issues, such as classification,[7] media leaks,[8] and foreign espionage[9]
- official government commission or task force reports that recommend fixes to deficiencies in secrecy.[10]

Notwithstanding the considerable virtues of most of the studies we examined, neither individually nor even collectively do they fully diagnose and prescribe treatment for the broad range of maladies that hobble a failing secrecy paradigm. Each identifies specific issues, but none examines the core problems in a way to identify and attack even most of them. The present literature on secrecy is encumbered by the absence of any conceptual framework with the theoretical power and reach needed to address the modernization of secrecy—not only classification issues but also safeguarding and disclosure—and synchronize it with the onerous requirements of the 21st century. Our use of the paradigm concept presents a basis for comprehensive theoretical insights into secrecy—defining the component parts and processes of secrecy, highlighting hidden relationships among these parts and processes, providing rigorous criteria to evaluate their performance, connecting the seemingly disconnected, and generating ideas and hypotheses to create evidence-based policy recommendations that can mitigate or reverse secrecy performance failings. Adopting this approach to examining secrecy requires the identification of paradigm content and boundaries that will focus attention on the chief performance components of secrecy management. We define the "secrecy paradigm" as *the combination of its elements—structure, culture, rules, and technologies—that shape or regulate the processes of classification, safeguarding, and disclosure of the nation's secrets.*

Abbreviations

CIA	Central Intelligence Agency
DNI	Director of National Intelligence
EO	Executive Order
FBI	Federal Bureau of Investigation
FOIA	Freedom of Information Act
IC	Intelligence Community
ISOO	Information Security Oversight Office
IT	information technology
NGA	National Geospatial-Intelligence Agency
ODNI	Office of the Director of National Intelligence
PCLOB	Privacy and Civil Liberties Oversight Board
PERSEREC	Defense Personnel Security Research Center
PIDB	Public Interest Declassification Board
SME	subject-matter expert

Paradigm Elements

The four elements included here—*structure*, *culture*, *rules*, and *technologies*—are intended to define both the key boundaries of the conduct of secrecy and the dynamics of human and technical engagement in its operations.

The *structure* of the secrecy paradigm refers to the principal institutions and organizations that carry out all or most of their work in secret or have major equities in the conduct and management of government secrecy. It also encompasses the shared power arrangements among these institutions and organizations, both within executive

branch organizations and between the executive and legislative branches.

The *culture* of the secrecy paradigm refers to the attitudes, values, and beliefs of government officials, stakeholders, observers, and relevant publics toward issues involving the classification and release of classified information. In some government organizational cultures, secrecy has high importance, while in others, secrecy requirements can often impede departmental business. Such differences illustrate a wide diversity of approaches to making, protecting, and releasing classified information.

The *rules* of the secrecy paradigm encompass the laws, EOs, regulations, and court decisions that bear on how government manages issues of secrecy. Prominent among these are several key statutes, the numerous EOs that provide broad policy guidance on secrecy management, program classification guides, declassification directives, and assorted nondisclosure agreements that employees typically sign as a condition of access to employment or classified information.

Finally, *technologies* of the secrecy paradigm are the newest element. The chasm between the primitive technologies of the formative stages of the secrecy paradigm and today's Information Age technologies marks the biggest change across the seven-decade span of post-war management of government secrets. Technology is a double-edged sword for both protecting and releasing secret information—it is a powerful force for modernization and information sharing, but it is also a potential master key to vaults of priceless information targeted by insider threats and foreign adversaries.

Paradigm Processes

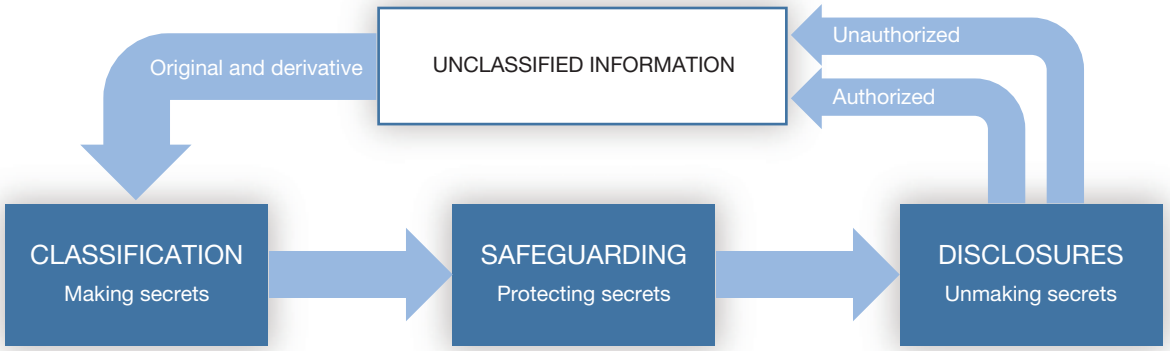
Processes are distinct from paradigm elements per se, but they are clearly influenced by them. Three connected processes capture the life cycle of secrets: how information becomes secret, how secrets are protected and transmitted, and how they become information that is no longer secret (Figure 1).

Classification: Secrets are created when information becomes classified as national security information at the levels of Confidential, Secret, or Top Secret by the act of authorized officials who believe that its disclosure could cause damage to U.S. national defense or foreign relations. This process is decentralized, with separate agencies deciding which of their information requires the protection that classification is intended to provide.

Safeguarding: Secrets are routinely protected in classified channels through such security measures as classified markings, special handling procedures, fences, safes and locks, computer passwords, and firewalled information technology (IT) systems. These measures, along with related restrictions designed to limit exposure of secret information to only those authorized to see it, are all intended to limit physical and electronic access.

Disclosure: Processes for disclosing secrets—breaking them out of routine classification protection and making them available to those who would not otherwise see them—can take two basic tracks. Authorized disclosures are officially declassified or shared secrets released through formal decisions of government. Unauthorized disclosures are secrets illegally released against government intent. Some unauthorized disclosures appear in the media as leaks of classified information, while others are obtained by foreign governments through espionage.[11] We address

FIGURE 1
Paradigm Processes: The Pathway of Secrets



issues of unauthorized disclosure under the safeguarding process of the paradigm and address authorized disclosure as its own paradigm process.

Evaluating the Secrecy Paradigm

Overall paradigm performance can be assessed on how well or poorly each paradigm element and process performs in satisfying its respective functions and goals.

Paradigm Elements: Evaluation and Recommended Remedies

How do the paradigm elements—structure, culture, rules, and technologies—affect the performance of the secrecy paradigm? If these elements hamper performance, what can be done to improve them?

Structure

The structure of the secrecy paradigm—i.e., the national security institutions that require secrecy for their work and the shared power arrangements among them—is a key driver in paradigm performance. These organizations include the 17 members of the IC, as well as significant non-IC components of the Departments of Defense, State, Homeland Security, Energy, Justice (including the Federal Bureau of Investigation [FBI]), and the White House. Other organizations include a second structural layer that advises or oversees the foregoing organizations on secrecy matters, such as the ISOO and the PIDB.

While these organizations operate with top-down guidance found chiefly in laws and EOs, secrecy execution is notably decentralized. This tension between centralization and the local autonomy that agencies exercise on a day-to-day basis reveals a problem that has grown in the

How Much Classified Information Is There?

No one knows. The Public Interest Declassification Board estimates that "[a]gencies are currently creating petabytes of classified information annually." One petabyte is the equivalent of approximately 20 million four-drawer filing cabinets' worth of paper (86 billion pages of textual data). This estimate is for the Intelligence Community (IC) alone and does not include information from the Departments of Defense, State, Homeland Security, and Energy.

Although we do not know the relationship between the actual amount of classified information and decisions to classify it, the Information Security Oversight Office reports that in fiscal year 2015 alone, executive branch agencies made a total of 55,245,608 classification decisions.

SOURCES: Public Interest Declassification Board (PIDB), *Transforming the Security Classification System*, Washington, D.C., November 2012, pp. 3, 17; Information Security Oversight Office (ISOO), *2016 Report to the President*, Washington, D.C., 2017, p. 1; and Harry Cooper, "Transforming the National Security Classification Process: A Perspective on the Way Ahead," *Transforming Classification: The Blog of the Public Interest Declassification Board*, blog, May 2011.

Information Age. The comparative simplicity of the immediate post–World War II era, during which the present paradigm was beginning to take shape—and during which secrets were far fewer and easier to protect—has given way to today's daunting complexity in classification and declassification and a notable rise in the difficulty of protecting information between those two decisions.

The secrecy paradigm operates with a distributed power arrangement that allocates secrecy responsibilities and authorities among the key participants. With the national government providing overarching guidance and direction, component agencies and elements execute the actions needed to protect secrets and move information into or out of the secrecy paradigm. This structural impact on secrecy is far reaching: What ultimately becomes secret is largely a matter of agency decisionmaking, as are actions affecting information protection and declassification. While EO-level guidance is straightforward, local execution produces a kaleidoscope of results. If the national-level policies seem uniform, actual implementation can produce wide diversity in outcomes, resulting in inadequacies in both protection and transparency.

Assessing "damage" is a case in point: The official rationale for classifying information is based on the degree of potential harm its loss could cause to the United States if divulged without authorization. However, EO 13526 provides no detailed explanation of how such damage should be determined. While these issues are sometimes covered in discrete classification guides, rigor and uniformity in execution can be elusive, even within a single agency. This necessarily leads to ambiguity and subjectivity in the localized classification process. These varied outcomes further complicate and confuse later declassification decisions (often nondecisions). The effects of ambiguity and subjectivity inherent in both classification and declassification are thus amplified by agency autonomy. For example, excessive decentralization may provide a poor framework for the greater protection of fragile sources and methods that remain a *sine qua non* for effective intelligence.

Evaluation of Structure

Structurally, excessive decentralization of agency-level decisionmaking about secrecy has contributed to overly complex, largely subjective classification and declassification decisions; poor definitions of key terms and concepts that hamper legitimate secrecy goals with their ambiguities and lack of rigor; and insufficient safeguarding measures, which permit unacceptable exposure and unauthorized disclosures of important secrets that need much greater protection than they currently receive. While substantial decentralization has its benefits, the lack of clearer, more-rigorous centralized direction has also contributed to excessively complex and varied classification outcomes, inconsistent protection for intelligence sources and methods, and lagging declassification and transparency. Reducing ambiguity and confusion resulting from local autonomy among agencies suggests that a review is needed of the way secrecy authorities are distributed within the executive branch—and that a greater oversight or legislative role for Congress is possibly necessary. Greater specificity can be achieved through more-centralized authorities that define, regulate, and manage the conduct of secrecy.

Recommended Remedies

Greater centralization and clarity in secrecy policy through a single policymaking designee or body with meaningful enforcement authorities can better address such interagency issues as classification and declassification guidance, uniform training and certification standards, IT systems, and other services of common concern. Within the IC, centralization could bolster enhanced protection of intelligence sources and methods. But more centralization in itself will be ineffective without a clear recognition that one size does not fit all, and perhaps should not, when different elements of government legitimately have different missions, needs, and cultures. Therefore, different agencies may be allowed different paths to achieve the same goals, so long as they are consistent with centralized direction.

Congressional consideration and potential enactment of a comprehensive secrecy and transparency statute accompanied by sufficient appropriations. Such legislation could establish a policy framework to provide much-needed guidance for all elements of government, to improve the government's ability to better protect classified information, and to improve governmental transparency by releasing secrets that no longer require classified protection. Such a law could establish policy and oversight requirements for successful secrecy, including establishing, while respecting presidential authorities, more-rigorous and -standardized criteria for identifying and protecting secrets as well as accountability for both the protection (e.g., antileaks legislation) and transparency (e.g., meeting declassification milestones) goals of paradigm performance.

Culture

The cultures of government organizations can be even more important in driving—or resisting—reform than the institutions themselves.[12] In matters of secrecy, organizational cultures vary widely. Some organizations are conflicted within by a cultural duality that simultaneously favors and opposes secrecy. For example, parts of the Department of Energy's workforce have favored open scientific inquiry and exchange of ideas, even with foreigners, while other parts of the department have opposed such

openness for reasons of protecting sensitive, often classified, nuclear secrets.[13] The National Imagery and Mapping Agency, now the National Geospatial-Intelligence Agency (NGA), was created in 1996 by merging secrecy-prone intelligence organizations with more-open mapping organizations that provided services for public aerospace and maritime navigation. These disparate cultures still frequently collide, with some staff pushing information sharing with mission partners and others resisting on secrecy grounds. Some evolution is evident in a trend toward openness, in which senior leaders are launching a number of initiatives to better manage these cultural conflicts. A notable example is reflected in NGA's new consolidated classification guide (discussed below).[14]

Two organizations illustrate contrasting cultures of secrecy and openness, and their different approaches mirror their different missions. The well-founded reputation of the Central Intelligence Agency (CIA) as highly secretive results in part from the clandestine nature of its mission to collect foreign intelligence through human espionage and hidden technical means and to conduct covert action influence operations. The Department of State, on the other hand, sometimes finds secrecy as an impediment to relations with foreign citizens, as discretion is valued but spying is not in the diplomatic tool kit. As one veteran of both organizations expressed it, "Unless you want a State Department so secure that it is ineffective, or a CIA that is so leaky that it is ineffective, these differences are a good thing."[15]

Dissimilar cultures also shape contrasting institutional positions on dealing with leaks of classified information. A seasoned intelligence officer, for example, argued that the fully cleared government officers who leak neither understand intelligence nor realize the damage their leaks might cause. The problem, he added, lies with giving too much classified information to too many others outside the IC, who then leak that information to unauthorized recipients, such as the press.[16] While no open-source research presents comparative data addressing the proportion of intelligence users (as opposed to intelligence producers) in the policy community who account for serious leaks, a journalist's study found that the primary government sources of serious leaks are senior political appointees, policymakers, and senior executives from executive branch agencies, along with members of Congress and their staffs.[17] Journalist Elie Abel cited data from a Harvard survey of former federal officials in policymaking positions in which 42 percent of those respondents acknowledged leaking classified information to the media. Abel characterized the majority of these unauthorized disclosures as "policy leak[s]."[18] A RAND Corporation study by two of the authors of this Perspective addressed the culture of leaking at the Department of Defense and noted that in the Department of Defense, as in other government organizations, much of the classified leaking is the result of a culture of acceptance and permissibility.[19]

Cultural issues also inhibit openness and transparency, contributing to overclassification. A 2012 report by the PIDB, for example, criticized the overall government culture of secrecy and lack of information sharing both inside the government and with the public, stating, "in its mission to support national security, [the government] keeps too many secrets, and keeps them too long; it is overly complex; it obstructs desirable information sharing inside of government and with the public."[20] Worse, according to the PIDB, overclassification is a consequence of having

an institutional culture of caution, with every incentive to avoid risk rather than to manage it.[21] According to one expert in classification and declassification issues, most classifiers have been culturally taught only to look for reasons to classify, not to look for reasons to leave something unclassified or to compose information with an uncleared audience in mind.[22] The Moynihan Commission's report urged adoption of a risk-management (instead of a no-risk) approach to classification decisions,[23] and the more recent study by the Brennan Center recommended that performance evaluation measures be used to change cultures and deter and hold accountable those who overclassify.[24]

Evaluation of Culture

Institutional cultures show great variation in attitudes and approaches toward secrecy, even within individual agencies. The principal flaws in the culture of secrecy concern the differing acceptability and limited understanding of widely disparate practices that highlight, if not exacerbate, ambiguities, inconsistencies, and divergence in how issues of secrecy are treated. Some reveal a cultural bias that favors overclassification and leans against transparency and declassification, while others may have a tendency to underclassify and have a more permissive attitude toward leaking. These differing practices in transparency and declassification also suggest that basic assumptions regarding secrecy are not universally shared. Little meaningful change is likely without addressing cultural dispositions toward secrecy.

Recommended Remedies

A concerted national-level leadership effort, supported by the National Security Council, to forge a common understanding of responsible and balanced secrecy reform—including greater transparency—among the culturally diverse organizations that make up the national security community. Cultural changes are much needed for agencies that operate largely in secret, and training is required to address attitudinal resistance to modernizing the secrecy paradigm.

According to one expert in classification and declassification issues, most classifiers have been culturally taught only to look for reasons to classify, not to look for reasons to leave something unclassified or to compose information with an uncleared audience in mind.

Specific training and education upgrades, including the development of a professional secrecy ethic as a core competency spanning both protection and openness goals; a zero-tolerance policy on leaking classified information; **mandatory training for classifiers, declassifiers, and users of classified information (including all new incoming officials) with annual certification requirements**; **a risk-management, rather than a no-risk, approach; and greater openness, including disincentives for overclassification**. We support the PIDB recommendation that training "should address cultural bias that favors classification, and often over-classification, through coordinated, consistent education that underscores the responsibility to not classify in the presence of doubt."[25]

Rules

Key rules of the secrecy paradigm guide and regulate permissible behavior for its practitioners. These rules address how information is classified and declassified, how personnel are vetted to handle classified information, and when information should be shared or protected.

In general, the rules involved in classification decisions are esoteric, agency-specific, and often unclear. Worse, according to an official knowledgeable about classification and declassification guidance, many of those who must follow them frequently do not understand why they are making the classification or declassification decisions they make.[26] In some agencies, those responsible for following the rules when they make classification decisions rarely interact with those who perform declassification, creating additional challenges when it comes time to evaluate whether material should remain classified.[27]

Perhaps the overriding criticism of secrecy rules is the lack of rigor and clarity in definitions and expectations; excessive subjectivity in rule implementation; and confusing and often conflicting guidance on what should constitute a secret, why secrets are kept, and how long secrets should remain protected. The result is a vastly more complicated and far larger body of classified information than perhaps intended by national-level EO guidance.

Rules for personnel vetting require serious review. The White House's recent focus on leakers and spies demonstrates that present vetting procedures are failing at some level, as some personnel who have been deemed trustworthy at an early point in their careers are not as trustworthy later.[28] The rules for vetting applicants and renewing existing clearances have failed to prevent major penetrations and compromises of classified information.

Finally, the emphasis on greater intelligence sharing since 9/11, however worthy, has resulted in confusion about which protected information can be shared and when. Interpreting what "responsibility to share" means[29]—especially when balanced against the contradictory "need to know" principle—is difficult. As interpreted by different managers and different agencies, these countervailing tensions produce confused or contradictory decisions about what to share and what to withhold. This area of uncertain guidance results in workforce puzzlement in more than one agency.

Evaluation of Rules

Rules affecting secrecy are often confusing and lack rigorous definitions, expectations, and enforcement. As a number of our interviewees asserted, much of the day-to-day rulemaking and execution in secrecy are arcane,

agency-specific, and unclear to employees.[30] Classification and declassification appear to follow different standards of secrecy. Rules for personnel vetting appear demonstrably inadequate in timely screening of the reliable workforce needed for improved protection of classified information. Important definitions are often poor, inconsistent, or absent. As one information management official put it, training is spotty and of mixed effectiveness.[31] Contradictory rules for information sharing and protection require deconfliction and greater clarity.

Recommended Remedies

Ensure that rules for classification and declassification are better connected and more rigorous, better define key terms, and clarify confusing language. A notable example of confusion is the definition of "harm" or "damage" when secrecy is compromised.

Review options for and enact a comprehensive national framework that defines the meaning of "national security." Currently, classification protections apply exclusively to information relating to national defense and foreign relations; this information is under executive branch control. Yet compromises in other information categories such as critical infrastructure vulnerabilities; power grids and ports; and sensitive information in banking, economics, agriculture, and energy could also damage national security if disclosed to hostile foreign entities. A statutory framework could establish policies, objectives, and priorities that reflect the importance of interests that are outside the current classification system but warrant protection.

Mandate a single, comprehensive classification guide to span an entire agency's classified activities, then seek more government-wide consistency across the new guides. The ambitious NGA consolidated security classification guide is an exemplar of a guide intended to enhance both protection and transparency goals. It provides rigorous guidance to determine the value of the information to be protected, the potential damage if disclosed, and how users can deal with specific classified information in an unclassified way.

Intensify the push for more-robust vetting rules for security clearances, including evidence-based and more-reliable predictive models of security trustworthiness. More research funding is needed to support a more analytical, evidentiary basis for a personnel vetting system that better suits the 21st century.

Ensure vigorous new and ongoing training and education programs that reinforce the vital role of rules and their enforcement and address human resources recruitment and screening of new applicants as well as intra- or interagency transfers and reassignments.

Technologies

As the PIDB has emphasized, technology has revolutionized the way information is created, stored, transmitted, and accessed.[32] Through our interviews, we found that there is much discussion of and interest in, as well as some ongoing development of, more-effective technology; however, there is still much more to be done. While technology can greatly improve classified information processing—such as improving the ability to classify, maintain, track, and sort certain kinds of classified material—it is neither widely used nor trusted for this purpose.[33] Cutting-edge technologies can help automate both classification and declassification through innovations in metadata use. However,

The development of the technologies needed for dramatic improvements in declassification (single-document analysis requiring the application of potentially thousands of rules to each and every document) are poorly incentivized by the government.

the massive amount of classified data, as well as a lack of resources for declassification, impede the government's ability to move information out of the secrecy paradigm.[34]

Similarly, the development of the technologies needed for dramatic improvements in declassification (single-document analysis requiring the application of potentially thousands of rules to each and every document) are poorly incentivized by the government. Properly resourced, better technology could reverse the mountainous backlog (see box on p. 21) in declassification and accelerate its capacity to meet even modest goals.[35] As one declassification expert explained, with rare exceptions, this kind of technology is not being developed. Until declassification programs are made a national priority with a funding element that can not be diverted elsewhere, there will be no real progress for many years.[36]

A related technological concern is the potential insider threat of downloading volumes of classified data onto a thumb drive or compact disc and removing the data from a secure facility undetected. The massive leaks by both Manning and Snowden, as senior IC leaders have described them,[37] involve literally hundreds of thousands of unauthorized disclosures and dramatically illustrate these vulnerabilities. A recent study has emphasized the growing role of information and communications technologies in both classified leaks and in espionage: Referring to "disclosures by the terabyte," the study notes that a "bureaucrat can hide a library's worth of documents on a key fob, and scatter them over the internet to a dozen countries during a cigarette break."[38] Without significant changes in both technology and policy, these vulnerabilities are likely to be with us for quite some time. As expressed by one expert,

> [t]he creation of massive electronic repositories filled with sensitive information, the need for millions of employees to access these systems, and the shift in policy to permit the widest possible access to information created a perfect storm that is leading to a catastrophic failure of the classification system.[39]

Continuous monitoring and continuous evaluation are recent government initiatives to improve the ability to deter and detect security risks to classified information through better auditing. Continuous monitoring focuses on IT systems and emphasizes communications, and continuous

evaluation focuses on personnel security. However, the potential contribution of modern technology to these vital functions remains vast compared with its actual use.[40]

Evaluation of Technologies

The weakest of the four elements, technology is seriously lagging in key areas of classification, protection, and declassification. The difference between the primitive technologies of the formative stages of the secrecy paradigm and today's Information Age technology is the biggest change across the seven-decade span of post-war management of government secrets. Meanwhile, government technology has not kept pace. The stunning heists of classified information by Manning and Snowden demonstrated dramatic technology failings, as well as many other protection breakdowns. Technology is at once a powerful force for helpful modernization and a source of harm if technological weaknesses enable foreign plundering of U.S. vaults of priceless information. Poorly funded and incentivized, much-needed cutting-edge technology development is presently underutilized to support enhanced classification, secrecy protection, and greater transparency—the principal goals of EO 13526—but the potential of such technologies for improving the adequacy of the secrecy paradigm is still quite substantial.

Recommended Remedies

Mandate technological innovation for classified information management to significantly elevate the role of technology to support better and more-efficient classification and declassification decisions. This will help control access to sensitive information to only those who need it and assist with better auditing of IT usage along with use of hard copy documents and such physical security devices as safes, locks, sensitive compartmented information facilities, and storage containers for soft and hard copies.

Ensure technological support for front-loading metadata. This innovation would seek to properly and consistently write guides into the machines that tag information and have those tags follow the information wherever it goes. This technological boost will greatly support later declassification decisions, thus assisting transparency.

Establish comprehensive technology planning for a next-generation secrecy paradigm. This can best be achieved through an interagency task force combining the best technologists, security professionals, and transparency advocates with a mandate to bring the pre–digital age secrecy paradigm squarely into the 21st century.

Paradigm Processes: Evaluation and Recommended Remedies

How do the paradigm processes—classification, safeguarding, and authorized disclosures—affect the performance of the secrecy paradigm? If they hamper performance, what can be done to improve them?

Classification

The U.S. government classifies information to protect the defense and foreign relations of the nation. Without some measure of secrecy, the security of the United States would risk unacceptable exposure and vulnerability. Yet the classification process is often inconsistent. The Moynihan Commission pointed out over 20 years ago that classification then was notable for "the absence of clear standards to gauge the need for and type of protection."[41] This

significant deficiency has almost certainly worsened. The reasons are deeply rooted, and some are systemic.

As noted, a key structural attribute of classification is that it is necessarily agency-based. As each unique fact or item is considered for classification, no one is better qualified to determine its level of classification than the agency that either produced that information or derived it from other classified information. An enormous amount of diverse information becomes classified through decisions that are largely *sui generis* to individual agencies. Thus, the decision process inevitably invites an inherent organization-biased subjectivity, producing a wide range of definitions of what constitutes a classified item; the level of classification assigned to the same type of information may vary from agency to agency. The result is that classification labels may not be reliable indicators of genuine sensitivity, nor of what should necessarily be classified.

Governmental struggles with overclassification have a long history. Current government data indicate that when declassification reviews are requested by the public, at least part of the document is released approximately 92 percent of the time.[42] This suggests that significant amounts of unclassified information are not accessible to the public until someone petitions to have the information released, potentially eroding public confidence in government classification practices.

The growth in classification decisions in the 20-year period of 1995–2015 has been dramatic. A comparison of the number of 1995 classification decisions in Table 1 shows that while original classification decisions almost doubled over the past two decades, derivative decisions have expanded by 148 times.

Possible consequences of unnecessary or excessive classification are impaired accountability and a decline in public trust. The Moynihan Commission argued that the public is left "uninformed of decisions of great consequence. As a result, there may be a heightened degree of cynicism and distrust of government."[43] A government records management official pointed out that a combination of classifying (or overclassifying) documents at a high rate and a lagging declassification system may create a serious process discrepancy, the impact of which may limit public understanding.[44] In addition, security classification has financial implications. A government estimate in 2010 put the figure spent on classification at roughly $10.8 billion, and this figure did not even include the efforts of some of the largest intelligence agencies.[45]

TABLE 1

20-Year Growth in Classification Decisions

	1995	2015	Growth
Original classifications	21,871	39,240	1.8 times
Derivative classifications	374,244	55,206,368	148 times
Totals	396,115	55,245,608	139 times

SOURCES: Data for 1995 are provided in Daniel Patrick Moynihan, *Secrecy: Report of the Commission on Protecting and Reducing Government Secrecy*, Washington, D.C.: U.S. Government Printing Office, 1997, p. xxxix. The 2015 data are from ISOO, *2016 Report to the President*, Washington, D.C., 2017.

Detailed guidance for making classification decisions is found in program- or agency-level classification guides, which vary greatly. In a notably innovative approach, NGA recently undertook an effort to eliminate its previous 65 guides and replace them with a single consolidated security classification guide. This superseding document aims to improve both protection and transparency by "building higher walls around fewer secrets." It produced a noteworthy 82-percent reduction in classified line items, removing more than 2,500 (mainly because of duplication and ambiguous statements), made 45 classification downgrades, and eliminated the Confidential category. It also explains why specific information is protected, describes the potential damage in the event of its disclosure, and guides users how to address classified items in unclassified ways.[46] With the promise of affording better protection when needed while facilitating greater transparency and information sharing, NGA's approach may help make a seemingly intractable problem tractable.

Evaluation of Classification

No truly standardized classification system exists to guide all agencies, and classification is characterized by unclear or confusing guidance and lack of rigorous standards. Inconsistencies abound. Different agencies and even different people can and often do classify the same information differently or even come to different decisions on whether to classify at all. Specifying damage-if-disclosed is a subjective and almost wholly conjectural process. Allowing that classification decisions are based on guidance, experience, reason, common sense, and caution—intended to be fair judgments, not wild guesswork—they are still, in the end, more subjective than not. Given the inherent institutional and cultural biases discussed above, any consequent overclassification—likely a frequent occurrence—impedes the goal of openness and transparency. The levels of projected harm from the unauthorized disclosure of classified information (damage, serious damage, and exceptionally grave damage for Confidential, Secret, and Top Secret, respectively) are neither authoritatively nor rigorously defined. There is no check on what classification labels really mean. This creates an environment in which there are potentially higher costs for underclassification because of greater exposure for sensitive information but no real penalties for overclassification; erring on the side of caution supports greater protection and does little discernible harm, as any reduction in potential transparency goes unnoticed. All this happens while the rate of classification is growing dramatically, with little or no connection between the classification and declassification processes.

Recommended Remedies

Evaluate the significant pros and cons of implementing the PIDB recommendation for a two-tiered classification system.[47] This approach, now introduced in NGA's new classification guide, would provide the strongest protection to Top Secret information, less protection to Secret information, and eliminate the present Confidential category.

Establish greater validity in classification decisions through more-explicit criteria and standards to ensure that information is appropriately classified and provide a clearer, sounder basis for subsequent declassification decisions. Such criteria should address the value of the information protected, the resulting damage of its compromise, and the level and duration of protection needed. In addition, clarify what is meant by requiring classifiers to

"identify" damage, as well as the "reasonable likelihood" that damage could result to national security.

Clarify what it means to balance protection versus disclosure by providing meaningful criteria and guidance for those who are involved in classification, including shelf life, through clearer policies, standards, and requirements relating to the duration needed for classified protection.

Distinguish intelligence information that must be classified because it would reveal a source or method from substantive information that can be shared more widely to ensure better-informed policymakers, legislators, and citizens. Require all classified information to be disseminated to users be prepared in **tear-line format** to easily distinguish what can be shared without risking compromise to sources and methods.

Develop better training and awareness about overclassification and common errors and train those who make them how to make better classification decisions.

Safeguarding

Protecting classified information is largely a security and counterintelligence function.[48] While the lion's share of this information appears to be well protected, and carelessness and human error are inevitable, significant cases of foreign espionage and unauthorized disclosures tell an alarming story: The United States isn't able to keep some of its most important secrets, and the implications of the damaging disclosures are often exceptionally serious and largely incalculable in dollars and in degraded intelligence, military, and diplomatic capabilities.

Espionage. The United States has long been a high-priority target of foreign adversaries, which recruit Americans in their efforts to steal U.S. secrets. Since the end of World War II, well over 200 Americans have been identified and prosecuted for committing espionage. Others have been caught but for assorted reasons have not been prosecuted. An unknown number have evaded detection or capture.[49]

Authoritative studies, such as those by Defense Personnel Security Research Center (PERSEREC), show that, since 1947, U.S. spies have provided, or tried to provide, classified information to 26 foreign countries and to al-Qaida. Russia (we include the the Soviet Union in this definition) has enjoyed the greatest success, with roughly 86 penetrations of U.S. national security organizations from 1947 to 2007. The former Warsaw Pact countries of East Germany, Hungary, Czechoslovakia, and Poland ran 29 U.S. spies; China ran 13; and Cuba ran nine. The loss of U.S. classified information due to these combined 137 penetrations can be described as wide-ranging and exceptionally damaging. As many as ten allied or friendly countries—such as Israel, the Philippines, and Taiwan—can also claim espionage successes against the United States.[50]

Although classified damage assessments have been conducted on most individual cases, with the exception of a single study conducted in the mid-1980s, we are unaware of any other comprehensive damage assessment of multiple spy cases, even just for major cases. Still, several notable cases are illustrative: The Walker (Navy) spy ring compromised key cards for enciphering messages and at least a million U.S. military and intelligence classified messages. The Conrad (Army) spy ring compromised Top Secret manuals on military communications and details of nuclear weapons and U.S. and North Atlantic Treaty Organization plans for moving troops, tanks, and aircraft.[51]

Spies Aldrich Ames (CIA) and Robert Hanssen (FBI) were just as damaging to U.S. intelligence. Ames compromised the identities of perhaps a dozen U.S. penetrations of the Soviet Union, at least ten of whom were executed; much of the U.S. double agent program against Russia; the tradecraft of agent operations and communications; ongoing technical collection operations; and hundreds of Top Secret intelligence analyses, including some scenarios of how the Russians could cheat on treaties. Hanssen went undetected for 22 years and compromised over 6,000 pages of classified documents, the identities of seven U.S. penetrations (three were executed), and details of many U.S. counterintelligence operations and of the most sensitive and highly compartmented IC and nuclear defense projects.[52]

Sixteen spies have passed highly damaging information on classified sources and methods pertaining to all four U.S. collection disciplines. When classified collection capabilities are compromised, major targets of U.S. intelligence can develop *denial* countermeasures to the exposed collection techniques, including enhanced counterintelligence against human intelligence collection, harder encryption and landline and courier transmissions against signals intelligence collection, and camouflage and concealment against imagery and geospatial intelligence collection. Adversaries with a detailed understanding of how U.S. intelligence works against them are better enabled to conduct *deception* against the United States by manipulating information and creating disinformation to spread through compromised channels. Unless such collected information is recognized as deceptive, it can influence U.S. analytical judgments provided to policymakers.[53]

Leaks. Unauthorized disclosures to the media that are published for the world to see, as former Director of Central Intelligence George Tenet told Congress, can be every bit as damaging as espionage.[54] The volume and seriousness of leaks have not abated since this gloomy characterization nearly 20 years ago. Rather, with the massive Snowden and Manning disclosures, abetted by WikiLeaks and other internet exposure, Tenet's alarm has become understatement. As with spy cases, detailed damage assessments remain classified. But we have learned much from reliable public sources to characterize some of the harm from serious leaks. The following cases represent the tip of the iceberg:

- **Snowden and signals intelligence.** Snowden exposed how the United States tracks terrorists via emails, social media, and cell phones. The director of the National Counterterrorism Center stated, "We've lost ability to intercept the communications of the key terrorist operatives and leaders. . . . We have specific examples of terrorists who have adopted greater security measures in the last year, including various types of encryption." An intelligence specialist noted that the leader of the Islamic State of Iraq and Syria (ISIS), Abu Bakr al-Baghdadi, had altered his communications to avoid detection. Electronic eavesdropping techniques used against al-Qaida in Iraq no longer worked. Based on Snowden's revelations, al-Qaida published a 7.5-minute video guide on the internet on how to avoid detection.[55]
- **9/11 and signals intelligence.** After the 9/11 attacks, U.S. intelligence was criticized for not providing better warning of al-Qaida's intentions. Referring to leaked intelligence supporting the 1998 cruise missile strikes against al-Qaida training camps in Afghanistan, then–White House Press Secretary

Ari Fleischer provided part of the explanation in a press conference: "[I]t was revealed publicly that the United States had [been intercepting] Osama bin Laden's satellite phone. As soon as it was publicly revealed, we never heard from that source again. We never again heard from that satellite phone. . . . That can damage America's ability to know important information that this government needs to protect the country."[56]

- **A CIA asset killed through press exposure.** Although his body has never been found, a CIA terrorist source is assumed to have been killed after an August 21, 1995, front-page article in the *New York Times*—despite the CIA's strenuous efforts to prevent publication—revealed his identifying details; the asset disappeared shortly after this exposure. His intelligence reporting on terrorism was judged to have been of incalculable value.[57]
- **Imagery and the surprise Indian nuclear tests.** Both authorized and unauthorized disclosures about intelligence techniques can be damaging. In this case, classified imagery had been used to support a diplomatic démarche asking India to stand down on its plans to test nuclear weapons in 1995; the imagery became the topic of press coverage based on leaked intelligence. The Indians then used countermeasures learned from these disclosures to prevent future satellite imagery from detecting signatures of preparation for their 1998 nuclear tests—and they caught the United States by surprise.[58]

Motivations for leaking include the political impetus to support or oppose policy, ego gratification, cultivating goodwill with the media, whistleblowing, and self-interest for personal or professional advantage; the activity is widespread.[59] Whatever the motive, some leakers have expressed the belief they are serving the public good and have tried to invoke whistleblower protection, regardless of the damage their leaking may have caused.[60]

Leaking classified information is illegal.[61] There are certainly many more leakers than spies, but they are rarely identified and held accountable for their crimes. During the period of 2005–2009, intelligence agencies filed 153 crimes reports of classified leaks to the press with the Department of Justice. However, only 24 leakers were investigated, only half were identified, and only a single indictment was issued.[62] The record improved markedly between 2009 and 2013, with seven successful prosecutions of leaking to the media, demonstrating that a determined government can establish legal accountability for unauthorized disclosures when investigations are pursued and successfully conducted.[63] Some legal experts argue that the present laws are ill-equipped to deal with leaks and should be revised.[64] Others have countered that the laws themselves are adequate but should be examined to determine whether comprehensive legislation to deal specifically with leakers provides a viable alternative.[65] It is clear, however, that those seeking to use criminal laws to deal with leakers face many obstacles—practical and legal—so that a review of the current legal system for dealing with leaks, whistleblower defenses, and freedom-of-the-press issues seems much in order.[66]

In sum, failures in the protection of government secrets can wreak untold and incalculable damage to U.S. national security. A major failing of the secrecy paradigm is its mixed performance in the prevention and detection of espionage, along with its inability to consistently deter,

apprehend, and hold leakers accountable for their violations of law.[67]

Evaluation of Safeguarding

A significant failing of the secrecy paradigm is its inability to protect classified information. As damaging as the more than 200 Cold War and post–Cold War espionage cases have been, classified leaks are arguably even worse, certainly in numbers and very likely in harm. These leaks are especially harmful in regard to intelligence sources and methods. The seriousness of these illegal breaches highlights the failure of the present secrecy paradigm to protect thousands of its most guarded secrets—many at the Top Secret level.[68] There is little reason to believe the situation will improve and, lacking any fundamental corrective measures, reason to expect it may get even worse.

The government's ability to properly protect classified information has almost certainly declined over time, owing to vulnerabilities in information and communications technologies that have been used for both unauthorized disclosures and espionage.[69] This decline probably correlates with the skyrocketing growth in the amount of secrets produced and with the correspondingly high growth in the numbers of people cleared to view classified information (now estimated at over 4 million).[70] The chronic inability to stem unauthorized disclosures from media leaks and foreign espionage presents the most convincing evidence of the failure of the present secrecy paradigm. The persistent success of spies and leakers, today rightly defined as "insider threats," constitutes a daunting challenge to the present means of protecting classified information, the effectiveness of which appears to be in rapid decline.

Recommended Remedies

Vigorously restore the need-to-know principle to curtail unneeded access which puts classified information at risk. This could require an interagency study to implement the principle throughout the cleared workforces. A task force chaired by the National Security Council, including senior-level stakeholder representatives, should seek to establish common standards for definitions and implementation.

Create an access management system that categorizes all classified information into finite areas of substantive knowledge.[71] Access to particular categories would be allowed only on the basis of an individual's need to know. Collectors and original classifiers would be required to bin newly created information into one or more of these categories. Every cleared national security professional and appropriate administrative staff would be authorized access to a limited number of bins, depending on job assignment and seniority; junior personnel would have access to only one or a few categories, and seniors would be permitted greater access, consistent with their responsibilities. In the access management system, the need-to-know criterion, defined specifically for every cleared employee by the employee's supervisor, would be rigorously enforced, and information access and usage would be regularly monitored and audited.

Consider reducing the large numbers of cleared government and contractor personnel.[72] Security clearances throughout the entire national security workforce need to be authorized with greater care and discrimination than in the past. Security experts need to reconsider the actual requirements for cleared employees through a zero-based review to determine who genuinely needs classified

information to conduct their work. Based on the numbers cleared and the determination of actual needs, the costs and trade-offs of a possible reduction can be systematically assessed. The rule of vigorous restrictions on the numbers of persons who are permitted access to especially sensitive information has proven to be a sound and successful principle for special access programs.

Reduce the large numbers of cleared personnel who have broad access to highly classified information—"broad access" is key, since the extent of harm by the most-damaging leakers and spies (e.g., Manning, Snowden, Hanssen, and Ames) was caused by their wide access to areas well beyond their legitimate need to know.

Establish uncompromising accountability for leaking classified information to the media and internet sites like WikiLeaks. Consider civil and criminal attributes of antileaks provisions in a comprehensive secrecy statute to enhance enforcement; seek ways to improve identification of anonymous leakers and unwavering implementation of sanctions through administrative, civil, and criminal law; and establish robust training to change the cultural tolerance for leaking from policy communities that leak.

Provide robust support for continued enhancements in U.S. counterintelligence. The recent counterintelligence upgrades need to be sustained without any diminution in priority, importance, or resources, and enhanced as needed.

Authorized Disclosures

Greater transparency into the otherwise secret workings of government is achieved through authorized declassification of documents and official release of publicly requested classified information under the Freedom of Information Act (FOIA). These procedures, designed for greater openness, are intended to enhance government accountability by reducing the amount of official information the government can shield from public view through classification. In the wake of the Snowden disclosures, the U.S. government gave increased attention to the need for increased transparency in programs that may have an impact on privacy of U.S. persons. The President's Review Group on Intelligence and Communications Technologies and the Privacy and Civil Liberties Oversight Board (PCLOB) reviewed various surveillance programs and made recommendations on measures the government could take to release more information and improve transparency about the programs.[73] Congress also legislated increased transparency measures in the USA Freedom Act, which made statutory reforms in 2015, a few years after the Snowden unauthorized disclosures began. The Office of the Director of National Intelligence (ODNI), on its own initiative, issued the Principles of Intelligence Transparency for the IC[74] and is now statutorily required to release an annual Statistical Transparency Report presenting statistics on how often the government uses certain national security authorities.[75]

What all this means for the government, in the end, is increased demands on the authorized disclosure process, which is a process that was already overburdened with requests and underresourced. Based on numerous interviews and on a joint RAND Corporation/American Bar Association workshop of experts and officials, we conclude that the government transparency efforts, however well-intentioned, are largely ineffective. Both declassification and FOIA efforts are significantly underresourced, low-priority, behind schedule, and falling further behind, suggesting that the rate and volume of declassification

can never come close to matching that of classification. Many interviewees and workshop participants agreed that government declassification efforts have not kept pace with operational realities and technological progress.[76] While the rate of classification and storage capacity for classified information has increased, the ability to declassify has not increased at anywhere near the same pace.[77] The work is intensive and slow, and decisionmaking rests upon individual reviewer choices, not decisions at the enterprise level.[78] The sheer volume of classified material makes proper and timely declassification difficult.[79]

Multiple interviewees highlighted the fact that classification and declassification review are handled by different groups in some agencies and therefore are inconsistently applied.[80] The knowledge of why the material was classified in the first place resides more with the original or derivative classifier than with the declassification authority reviewing the material. In addition, declassification is almost never considered in a significant way when classification is decided.[81] There has been a push in parts of some agencies to write reports prepared for release from the beginning of the classification process, but this "front-loading" adds time to the production of classified material at the beginning of a process, frequently competing with short timelines and operational demands.[82] One IC interviewee pointed out that authorized disclosure work is extremely resource-constrained and that disclosure processes differ agency by agency, with no consistency. With so much agency decentralization in classification, and no real effort to connect the classifiers with the declassifiers, scheduled automatic declassification will be greatly slowed by necessary labor-intensive review. As explained by one declassification expert, "When things finally go up for automatic declassification, it's going to be worse. We could front-load this work, but agencies won't do it."[83]

The Near-Impossible Challenge of Declassification: Mountainous Backlog, Resource Canyon

"At one intelligence agency alone, it is estimated that approximately one petabyte of classified records data accumulates every 18 months. One petabyte of information is equivalent to approximately 20 million four-drawer filing cabinets filled with text, or about 13.3 years of high-definition video.

Under the current declassification model, it is estimated that one full-time employee can review *ten four-drawer filing cabinets of text records in one year*. In the above example, it is estimated that one intelligence agency would, therefore, require *2 million* employees to review manually its one petabyte of information each year. Similarly, other agencies would hypothetically require millions more employees just to conduct their reviews."

SOURCE: PIDB, *Transforming the Security Classification System*, Washington, D.C., November 2012, p. 17. Emphasis in the original.

Several interviews suggest that what is often deemed available for automatic declassification may not be declassified at the expected time for a variety of reasons. A workshop participant stated that very little that is supposed to be automatically declassified has actually been released.[84] A key reason for this is a lack of manpower and resources.[85] As one interviewee said, "Automatic declassification isn't automatic. There's not enough staffing to handle the requirements of declassification."[86]

One declassification official asserted that technology can aid the declassification effort; a pilot initiative that uses natural-language processing may work well in declassifying material. Such technology seems promising to help clear the backlog, as it requires a manual quality check but not necessarily a full interagency review process.[87] However, individual agencies, with their varying resources and capabilities, are unlikely to invest in and deploy this technology individually anytime soon.

FOIA is another measure that encourages agencies to be more proactive in authorized disclosure. Interviewees and workshop participants agreed that FOIA serves an important purpose supporting transparency. One interviewee noted that the large majority of requests come from a small number of politically driven petitioners who are responsible for much of the time-consuming work, backlogging the system and resulting in further delays for occasional petitioners, who have to wait in line far longer while massive requests overwhelm the capacity for judicious review.[88] Similarly, one workshop participant said that nuisance requests are problematic because they take effort away from public-interest releases and that agencies should prioritize declassification efforts based on historical or other significance.[89] Several workshop attendees believed that FOIA offices would need massive expansion to be fully functional.[90]

Another issue in declassification and FOIA release is prematurely or inadvertently placing still-classified information into the public domain. The problem of authorized disclosures potentially causing damage to intelligence collection sources and methods was identified by the Silberman-Robb Weapons of Mass Destruction Commission.[91] A Chinese intelligence publication identified a particularly egregious case, in which the Department of Energy declassified roughly 1.5 million items of nuclear materials. As the Chinese study explained it:

> They reviewed a total of 388,000 documents in 33 days, so each reviewer had to review around 1,000 documents a day, about two a minute. The pace of the reviews was startling, and resulted in a large number of errors. . . . [S]ome 19,400 documents were mistakenly declassified, and of these there were at least eight highly secret items regarding thermonuclear weapons.[92]

Evaluation of Authorized Disclosures

The process for declassification and FOIA releases requires major overhaul and fundamental changes to improve openness and transparency performance to acceptable standards. There appears to be a consensus that the declassification system is overwhelmed and cannot realistically meet even modest expectations. The growth of classified information is quickly outpacing the capacity to later declassify it. The present approach to declassification and FOIA releases is failing in some ways because it is significantly underresourced, technology-deficient, and overwhelmed by a staggering workload that is poorly prioritized. If transparency goals are to be achieved, the process for achieving them will require major reforms and a significant infusion of much-needed resources.

Recommended Remedies

Accelerate and maximize needed efficiencies in declassification through closer coordination between classification and declassification processes and incorporation

of cutting-edge information management technologies to reduce the costly dependence on inefficient human-centric, labor-intensive processes.

Identify historically significant topic areas to focus declassification efforts on more meaningful topics to better satisfy a broader public interest, which could also improve cost effectiveness.[93]

Refine or eliminate automatic declassification of certain categories of information, such as intelligence sources and methods; consider establishing new proscriptions that limit high-volume requestors under the FOIA from monopolizing agencies' time and resources at the expense of other, less well-financed requestors.

Institutionalize and expand ongoing consultations between classifiers and declassifiers to ensure a continuity of understanding of what can safely be released for improved transparency and what requires continuing protection to avert damage to national security.

Clarify the rationale for continued classification of information that has been previously disclosed publicly, albeit not officially, and is an open secret.

Integrate an explicit counterintelligence perspective into disclosure decisions to minimize potential damage to national security by prematurely releasing information that should remain classified.

Implementation

The range of proposals presented here to improve the paradigm's performance can be tested in smaller pilot studies before sweeping reforms are implemented in full force. A more graduated approach could establish a policy "test bed" in which a variety of new secrecy reforms could be tried experimentally and on a small scale. This way, they could be validated or invalidated in practice before full implementation.[94] Also, the government should periodically reassess secrecy goals; review why the policies, standards, and practices relating to secrecy were established; and make changes when they are no longer current, effective, or needed in accomplishing valid secrecy objectives. Our recommendations range from easily accomplished tweaks in the paradigm elements and processes to considering new legislation for a whole-of-government approach, with many efforts that fall in between these poles. A comprehensive secrecy and transparency statute could better define what national security means in the Information Age, design a classification framework that would include more than just government documents and couple classification with declassification, and craft antileaks provisions to address a long-standing failure in secrecy protection where little else has worked. This approach combines executive and legislative efforts that are intended not only to improve the paradigm but also to provide the foundation for a wholesale secrecy paradigm shift.

> "Striking the critical balance between openness and secrecy is a difficult but necessary part of our democratic form of government. Striking this balance becomes more difficult as the volume and complexity of the information increases."
>
> SOURCE: Barack Obama, "Implementation of the Executive Order [13526], 'Classified National Security Information,'" memorandum, Washington, D.C., December 29, 2009.

Paradigm Shift: Path to Secrecy Modernization

A prerequisite for striking that critical balance between openness and secrecy should be actually accomplishing these two goals with something close to passing grades—something not evident in the last century's secrecy paradigm. Transitioning to a 21st-century version that can achieve and balance both goals requires a clear understanding of why a secrecy paradigm designed for an earlier age comes up short on most measures necessary to smartly classify, protect, and disclose national security secrets in the Information Age. The paradigm concept puts these deficiencies into focus.

Diagnosing Failure

A key conclusion of this Perspective is that *much of the secrecy paradigm failure is rooted in the interdependency of its processes and elements*. Once the nature and impact of shortfalls in the paradigm elements are grasped, failing processes should come as no surprise. Because poorly performing elements necessarily diminish the performance of its processes, significant improvements in classification, protection, and disclosures cannot be achieved without corresponding correctives in the structure, culture, rules, and technologies that affect the processes of the secrecy paradigm. This is a powerful relationship (see Table 2). Its implications are that remedies applied to the paradigm processes alone without corresponding attention to the deficits identified in the paradigm elements are certain to come up short. More-effective and more-durable correctives to a faltering secrecy paradigm will require concerted attention to both elements and processes, and to their symbiotic relationship. Success (or failure) in one is the best predictor of success (or failure) in the other.

Engineering a Paradigm Shift

A fully modernized 21st-century secrecy paradigm cannot be achieved without coming to grips with what it will take to transform the old one. Sound understanding of its frailties and fault lines is foundational to the task. Knowing what a genuine 21st-century paradigm should look like will help navigate the transition between them.

Managing secrecy is a whole-of-government issue. No single agency or department of government, or even branch of government, presently has the capacity, the responsibility, or even the will to address, much less correct, the most-serious problems—many of them systemic—contributing to paradigm failure. This is because of the wide scope of secrecy that spans every U.S. national security organization, the importance of the issue, the potential effects of failed secrecy on the security of the nation, and even the functioning of U.S. democracy related to openness and accountability. It is increasingly clear that modernization is a critical, even an urgent, national imperative. Achieving modernization will require a paradigm shift to accomplish this. A transition between two paradigms—one from the last century and the other for this one—will require a shift in the present allegiances of secrecy practitioners, as Kuhn suggests. As we have identified little in the way of strong allegiances to the status quo, perhaps a genuine paradigm shift is not the impossible task it might seem.

TABLE 2

Diagnosing Failure: The Paradigm Insight

	Structure	Culture	Rules	Technology
Classification process	Excessive decentralization and agency autonomy necessarily yield excessive complexity and confusion in classification procedures and decisions.	An inherent cultural bias in many agencies pushes classification or overclassification when less protection may be warranted.	The general lack of rigor in classification/declassification rules and lack of discipline in their application results in a high degree of subjectivity and variability of standards in classification decisions.	The aspiration for greater automation in classification decisions remains a distant goal, impeding progress toward greater efficiencies and government-wide classification standardization.
Safeguarding (protection) process	Greater secrecy protection can be realized through stronger and more-centralized authorities, and possibly also through antileaks legislation. For the IC, a top-level (Director of National Intelligence [DNI] or principal deputy DNI) push for improved protection for intelligence sources and methods—especially for those that are fragile and perishable—can strengthen protection for the most-vulnerable and costly capabilities at risk through unauthorized disclosures.	The lax culture toward leaking among intelligence consumers and users of intelligence (not primarily intelligence-producing agencies) represents a major impediment to better protection of sensitive and perishable sources and methods, as well as sensitive military capabilities.	Strengthening weak enforcement of dated laws that prohibit leaking and poor personnel-vetting procedures can greatly improve the safeguarding of classified information, along with vigorous restoration of the need-to-know principle and establishment of a strict access management system.	Cutting-edge technologies that can audit unauthorized access and disclosures through continuous monitoring and continuous evaluation remain far from full development and implementation. Once deployed, significant upgrades in secrecy protection can much enhance personnel vetting and IT vigilance.
Disclosure process	Significant decentralization in classification impedes declassification by amplifying the disconnectedness between the two processes. Declassification accuracy and efficiencies can be much enhanced through closer engagement with original and derivative classification decisions and processes, in particular, through more front-loading engagement.	Cultural attitudes of some management and much of the workforces in many IC agencies and Department of Defense components favor safeguarding disproportionately over transparency, often subtly encouraging greater classification. Such attitudes tend to resist policies favoring openness and sustain underresourced conditions for lagging declassification programs, technologies, and efforts.	Rules generally tend to favor classification over declassification and release, and rules for declassification tend to be weaker and less well enforced. The combination results in a significant and mounting backlog of declassification work and diminished production and release.	Powerful information management technologies that can couple classifiers with declassifiers and accelerate declassification are needed but poorly resourced and lagging in development, resulting in delayed or reduced production and release of declassified materials.

Paradigm shift—"An important change that happens [to a paradigm] when the usual way of thinking about or doing something is replaced by a new or different way."

SOURCE: *Merriam-Webster Dictionary*, 2018.

Paradigm shift—A transition between competing paradigms [characterized by] an increasing shift in the distribution of professional allegiances.

SOURCE: Thomas S. Kuhn, *The Structure of Scientific Revolutions*, 3rd ed., Chicago: University of Chicago Press, 1996.

What a Paradigm Shift Must Entail

Correctives for the failings we have identified would, rather than tinkering at the margins, seek significant modernization and improvements in every paradigm element and process examined. Whatever specific actions policymakers decide to implement, a paradigm shift would demonstrate the following attributes to improve performance, inspire confidence, and further U.S. national security imperatives:

- comprehensive reform that provides a whole-of-government framework for identifying national security interests that require secrecy protections and establishing legislative and executive branch roles and responsibilities for overseeing and managing the protection of national security information in the Internet Age
- a new structure that finds a better balance between enforcing centralized policy roles and enabling decentralized implementation of national policies and objectives
- a culture that values and reinforces more evenly that protection and disclosure are significant public interests—a shift that would help move elements of the national security community and consumers of their products toward both improved security and transparency through sound policy, education, and accountability
- rules that reduce classification subjectivity to provide greater classification validity to similar information; provide rigorous definitions with standardized, clear criteria, including specific damages anticipated from disclosure; and impose reasonable requirements and sanctions for transgressions to enhance compliance
- technologies that aggressively incorporate 21st-century information management capabilities and related digital-age tools to better regulate access to classified information based on need-to-know principles, and to assist in classification and declassification decisions
- a classification system that more rigorously establishes criteria for determining damage and better connects it to the need for protection, weighing the benefits and costs of protection versus disclosure in implementing the PIDB-recommended two-tiered approach. Such a system would also better connect decisionmaking in classification and declassification. In intelligence, classification will better distinguish between information content that can be sharable, particularly for public policy debate, and

their sources and methods, which require continued protection for effectiveness.
- a safeguarding function that implements a need-to-know framework to strictly limit access to classified information, evaluates the feasibility of a reduction in the numbers of cleared personnel, and fully implements audit and monitoring programs. Its unauthorized disclosure remedies would encompass comprehensive antileaks legislation to clarify legal boundaries and accountability, distinguish leaking from espionage, define legitimate whistleblower interests, and establish an end-to-end accountability process to identify and hold leakers of classified information responsible for their damaging disclosures.
- authorized disclosure processes that prioritize historically significant information through a topic-based approach to reduce the growing backlog of declassification releases. To help minimize potential damage to national security by prematurely releasing information that should remain classified, new procedures would infuse an explicit counterintelligence perspective into the disclosure processes, foreign intelligence sharing, and diplomatic démarches that use classified information.

The central challenge faced by modernization of the U.S. secrecy paradigm is at its core the inability to identify and protect vital information—secrets—and to effectively distinguish information that does not need such protection. Effective governance in national security requires a fully functioning secrecy system for maximum possible effectiveness of the United States' military, intelligence, diplomatic, homeland security, and economic capabilities. This system must also provide greater transparency and better public access to information that can shed appropriate light on what is behind the secrecy door. Through our broad examination of the elements and processes of the present, dated secrecy paradigm, we have identified significant flaws in the way secrecy is conducted in the United States. The present secrecy paradigm neither protects nor releases national security secrets consistently or well, despite the long-standing aims of the paradigm and the clear intent of EO 13526 to meet these daunting twin objectives.

This Perspective has sought to identify both the seriousness of the problem and needed correctives to enable a paradigm shift to implement necessary change. Some of these changes are overdue at least since the Moynihan study urged similar reforms three decades ago; others are urgently needed to prevent further loss of information through technology advances—e.g., cyber attacks—for which the present paradigm was neither designed nor seems sufficiently adaptive. We are heartened by the inclusion of language in the now-passed 2017 FISA Amendments Reauthorization Act that requires the comptroller general to conduct a study of the classification system and protection of classified information, and are hopeful it will compel the U.S. government to take a hard look at the failures in the current paradigm. The overriding challenge is to ensure the nation's secrets are better secured and its values of transparency and openness appropriately maintained and advanced.

Appendix: Study Methodology

This Perspective reflects the analysis, findings, and recommendations reached during the authors' extensive study of current secrecy practices and their effects on national security. The methodology of this study is described in this appendix.

Data gathering and analysis. Adapting Thomas Kuhn's use of "paradigm" as the conceptual framework for the study, we acquired the needed information to evaluate the secrecy paradigm in three data-gathering approaches:

1. Expert opinion and data generated during in-depth interviews with 25 government officials and other experts and stakeholders, based on an extensive questionnaire developed for this study.
2. Consideration of a wide range of perspectives—both critical and supportive of the current secrecy system—discussed at a one-day workshop on secrecy co-sponsored by the RAND Corporation and the American Bar Association's Standing Committee on Law and National Security. This workshop brought together 40 senior officials and seasoned experts in security and classification issues.[95] Both the interviewees and the workshop participants were promised confidentiality to encourage their speaking candidly regardless of their current or former positions or status.
3. A review of official documentation and relevant literature that addresses governmental secrecy in the United States.

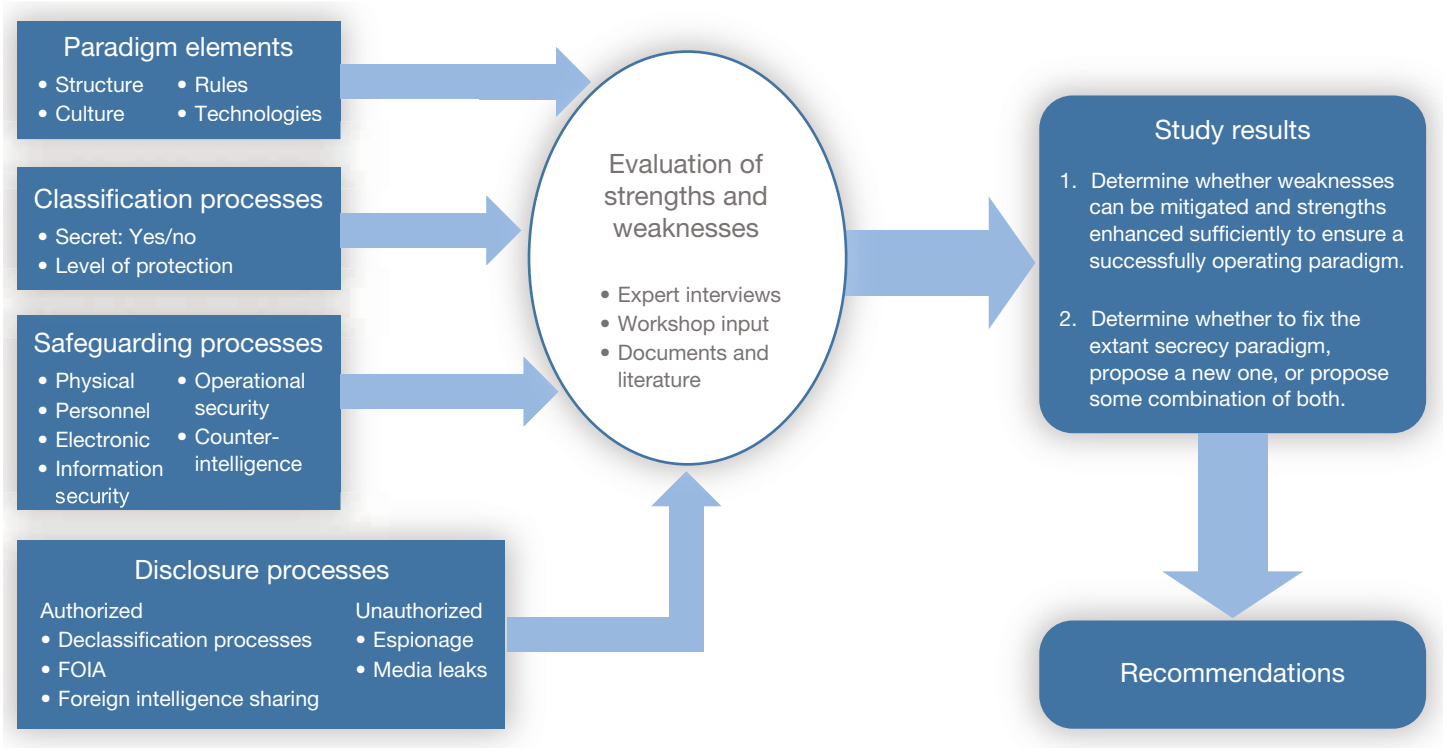
The basic design of the study is depicted in Figure 2.

The interviewees and workshop participants were selected to participate in the study because they are experts and/or stakeholders in the secrecy paradigm. Many are present or former senior government officials; others are academics, national security lawyers, or consultants whose expertise may be based on practitioner experience, research or advocacy interest, or a combination of these. Inclusion of these expert and stakeholder views uses a methodology consistent with qualitative research and does not purport to be a random or probability sample aiming to statistically generalize about or estimate characteristics of a larger population based on a smaller sample of respondents.[96] Its purpose is to identify and gather expert opinion across a range of views on such arcane topics as secrecy, in which public opinion surveys are of limited value in providing the kind of information sought.

Each of the 25 interviewees (whose anonymity is ensured through approval procedures of RAND's Human Subjects Protection Committee) agreed to an approximately one-hour, in-depth interview. They were selected from an initial list of about 80 names considered in project team discussions by identifying experts on the topic of the study with an eye toward ensuring a broad and diverse range of opinion among them. Most who agreed to and were available for interviews were either at that time, or had been, senior-level government practitioners; some were known professionally to the authors, while others were selected by reputation or by the positions they held presently or earlier.

The 40 workshop participants were promised nonattribution through Chatham House rules. They were selected in collaboration with the workshop co-sponsor, the American Bar Association's Standing Committee on Law and National Security, on the basis of the same expertise or stakeholder criteria. Half were selected by the RAND Corporation and half by the American Bar Association's

FIGURE 2
Paradigm Evaluation



Standing Committee. Like the RAND Corporation, neither the American Bar Association nor its Standing Committee has an editorial position on the study topic.

Our analysis of interview data followed objectivity procedures: Data acquired in these interviews were sorted and coded in a process derived from grounded theory.[97] Here individual responses are treated as standalones, then key themes and concepts are identified; the responses are then aggregated to find patterns in the themes and concepts that multiple respondents provide. These are then highlighted and compiled in a working document containing important quotes or concepts. The relevant quotes and ideas are then incorporated into the report where they bear on the study questions and issues. We supplemented these data with relevant observations generated in commentary voiced during the one-day secrecy workshop and with appropriate documents and literature surveyed during the course of the study.

Notes

[1] Former DNI James Clapper testified before the Senate Select Committee on Intelligence at a hearing titled "Current and Projected National Security Threats Against the United States" on January 29, 2014, and called threats to national security from insider threats "critical" and "potentially the most massive and most damaging theft of intelligence information in our history." See Kimberly Dozier and Stephen Braun, "U.S. Official: Snowden Leaks Lead to Pentagon Change," Associated Press, February 4, 2014. Then-President Barack Obama said, "If any individual who objects to government can take it into their own hands to publicly disclose classified information, then we will not be able to keep our people safe, or conduct foreign policy. Moreover, the sensational way in which these disclosures have come out has often shed more heat than light, while revealing methods to our adversaries that could impact our operations in ways that we may not fully understand for years to come." See Office of the Press Secretary, White House, "Remarks by the President on Review of Signals Intelligence," webpage, January 17, 2014. As of August 23, 2018: https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

[2] Steven Aftergood, "Intelligence Transparency to Build Trust: A Postscript," *Federation of American Scientists*, April 5, 2018. As of August 23, 2018:
https://fas.org/blogs/secrecy/2018/04/transparency-trust-postscript

[3] Thomas S. Kuhn, *The Structure of Scientific Revolutions*, 3rd ed., Chicago: University of Chicago Press, 1996.

[4] "Classified National Security Information," Washington, D.C.: Executive Office of the President, Executive Order 13526, December 29, 2009. As of August 23, 2018: https://www.federalregister.gov/documents/2010/01/05/E9-31418/classified-national-security-information

[5] Daniel Patrick Moynihan, chairman, *Secrecy: Report of the Commission on Protecting and Reducing Government Secrecy*, Washington, D.C.: U.S. Government Printing Office, 1997, p. xxi. The commission's report is generally referred to as the Moynihan Commission Report. See also Edward A. Shils, *The Torment of Secrecy*, Chicago: Ivan R. Dee, Inc., 1996; and David Wise and Thomas B. Ross, *The Invisible Government*, New York: Bantam, 1965.

[6] Moynihan's co-chairman, Congressman Larry Combest, endorsed the report but argued that the importance of secrecy outranks reducing security measures. "Protecting National Security Secrets in a 'Culture of Openness,'" in Moynihan, 1997, pp. xlvii–li. Gabriel Schoenfeld presents a well-argued post-9/11 defense of secrecy in *Necessary Secrets: National Security, the Media, and the Rule of Law*, New York: W.W. Norton, 2010.

[7] Harry Cooper makes a compelling case that "nothing short of a complete overhaul will fix classification" in Harry Cooper, "A New Approach to National Security Classification," white paper, June 2017. As of September 10, 2018: https://fas.org/sgp/eprint/cooper-nsi.pdf
Arvin Quist has produced a substantial guidance manual on classification in *Security Classification of Information*, Vol. 2: *Principles for Classification of Information*, Oak Ridge, Tenn.: Oak Ridge National Laboratory, April 1993. Martin Libicki et al. attempt to offer a "general framework for judging classification decisions," in Martin C. Libicki, Brian A. Jackson, David R. Frelinger, Beth E. Lachman, Cesse Cameron Ip, and Nidhi Kalra, *What Should Be Classified? A Framework with Application to the Global Force Management Data Initiative*, Santa Monica, Calif.: RAND Corporation, MG-989-0JS, 2010. As of August 23, 2018: https://www.rand.org/pubs/monographs/MG989.html
The study sets the classification bar unreachably high for classifying intelligence and other sensitive materials and makes unwarranted assumptions about what can be known about foreign exploitation of publicly available information that should be classified. Like Moynihan, Elizabeth Goitein and David M. Shapiro fault overclassification for eroding democratic government by inhibiting public debate in *Reducing Classification Through Accountability*, New York: Brennan Center for Justice at New York University School of Law, 2011.

[8] See David E. Pozen, "The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information," *Harvard Law Review*, Vol. 127, No. 2, December 2013, pp. 513–635; Paul Rosenzweig, Timothy J. McNulty, and Ellen Shearer, eds., *Whistleblowers, Leaks, and the Media: The First Amendment and National Security*, Chicago: American Bar Association, 2014; Elie Abel, *Leaking: Who Does It? Who Benefits? at What Cost?* New York: Priority Press Publications, 1987; Gary Ross, *Who Watches the Watchmen: The Conflict Between National Security and Freedom of the Press*, Washington, D.C.: National Intelligence Press, 2011; James B. Bruce, "Laws and Leaks of Classified Intelligence: The Consequences of Permissive Neglect," *Studies in Intelligence*, Vol. 47, No. 1, March 2003, pp. 39–49; and James B. Bruce and W. George Jameson, *Fixing Leaks: Assessing the Department of Defense's Approach to Preventing and Deterring Unauthorized Disclosures*, Santa Monica, Calif.: RAND Corporation, RR-409-OSD, 2013. As of August 23, 2018: https://www.rand.org/pubs/research_reports/RR409.html

[9] See Michael J. Sulick, *American Spies: Espionage Against the United States from the Cold War to the Present*, Washington D.C.: Georgetown University Press, 2013; Katherine L. Herbig, *The Expanding Spectrum of Espionage by Americans, 1947–2015*, Monterey, Calif.: PERSEREC, 2017; and PERSEREC, *Espionage and Other Compromises of National Security: Case Summaries from 1975 to 2008*, Monterey, Calif., 2009.

[10] In addition to the Moynihan Commission, the most important of these reports—all well done but largely ineffectual in driving reform—are the 1955 Wright Commission on Security and the 1970 Seitz Task Force on Secrecy; summarized in Moynihan, 1997, pp. xxii–xxiii, A-61, G1, and G-2. The more recent commission on Iraqi weapons of mass destruction addressed secrecy issues as they bear on intelligence. See Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States*, Washington, D.C.: U.S. Government Printing Office, 2005, pp. 380, 436, and 545–546.

[11] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005, pp. 380–384.

[12] James Q. Wilson, "Thinking About Reorganization," in Roy Godson, Ernest R. May, and Gary Schmitt, eds., *U.S. Intelligence at the Crossroads: Agenda for Reform*, Washington, D.C.: Brassey's, 1995, pp. 28–35.

[13] President's Foreign Intelligence Advisory Board, *Science at Its Best, Security at Its Worst: A Report on Security Problems at the U.S. Department of Energy*, June 1999, p. 11.

[14] Discussion with security official and follow-up correspondence, July 19, 2017.

[15] Mark Stout, "Were Hillary's Emails Classified? Where You Stand Depends on Where You Sit," *War on the Rocks*, March 8, 2016.

[16] Interview with a senior intelligence officer, February 5, 2016, and follow-up correspondence.

[17] Abel, 1987.

[18] Cited in Ross, 2011, pp. 74–76.

[19] Bruce and Jameson, 2013, pp. 13–16.

[20] PIDB, *Transforming the Security Classification System*, Washington, D.C., November 2012, p. 2.

[21] PIDB, 2012, p. 9.

[22] Correspondence with U.S. government records management official, August 4, 2017.

[23] Moynihan, 1997, pp. 20–22, 52–53.

[24] Goitein and Shapiro, 2011.

[25] PIDB, 2012, p. 3.

[26] Interview with former IC official, May 25, 2016.

[27] Interview with IC official, May 20, 2016.

[28] White House, "Memorandum on the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs," Washington, D.C., November 21, 2012.

[29] A major shift in previous protectionist emphases, introduced by DNI Mike McConnell following the 9/11 and Iraq weapons of mass destruction criticisms, directed the need for significantly greater intelligence sharing.

[30] From multiple interviews, including with a U.S. government records management official, May 31, 2016; a U.S. government records management official, May 23, 2016; an IC official, May 20, 2016; and a former IC official, May 25, 2016.

[31] Interview with U.S. government records management official, May 23, 2016.

[32] PIDB, 2012, p. 25.

[33] Interview with U.S. government records management official, May 23, 2016.

[34] Interview with IC officials, April 26, 2016, and May 3, 2016.

[35] See PIDB, 2012, p. 17.

[36] Harry Cooper, correspondence with the authors, August 15, 2017.

[37] See Dan Verton, "Snowden Leaks 'Most Massive and Most Damaging' in History, Intelligence Chiefs Say," *Fedscoop*, January 30, 2014. As of August 23, 2018: https://www.fedscoop.com/snowden-leaks-massive-damaging-history-intelligence-chiefs-say; Clapper characterized the Snowden and Manning leaks as "massive" and described "WikiLeaks and the continued hemorrhaging of leaks in the media" as counterproductive to the DNI's goals for integration and collaboration the IC (James Clapper, remarks at 2010 Geospatial Intelligence Symposium, New Orleans, La., November 2, 2010. As of August 23, 2018:

https://www.dni.gov/files/documents/Newsroom/Speeches%20and%20Interviews/Clapper_GEOINT_2010.pdf).

[38] Herbig, 2017, pp. 162–163, citing Scott Shane, "Keeping Secrets Wiki-safe," *New York Times*, December 11, 2010.

[39] Cooper, 2017, p. 9.

[40] For continuous evaluation, see ODNI, "Continuous Evaluation—Overview," webpage, undated. For continuous monitoring, see CIO.gov, "Continuous Monitoring," webpage, undated. As of August 23, 2018: https://www.cio.gov/agenda/cybersecurity/continuous-monitoring; and Office of Management and Budget Memorandum 14-03, *Enhancing the Security of Federal Information and Information Systems*, Washington, D.C., November 2013.

[41] Moynihan, 1997, p. xxiv.

[42] Goitein and Shapiro, 2011.

[43] Moynihan, 1997, p. 8.

[44] Correspondence with a U.S. government records management official, August 4, 2017.

[45] Goitein and Shapiro, 2011, p. 11.

[46] NGA, "The Consolidated NGA Classification Guide (CoNGA)," briefing, July 20, 2017.

[47] PIDB, 2012, pp. 2–3, 13.

[48] This section draws from James B. Bruce, "Keeping U.S. National Security Secrets: Why Is This So Hard?" *The Intelligencer*, Vol. 22, No. 2, Fall 2016, pp. 47–54.

[49] PERSEREC, 2009; Katherine L. Herbig, *Changes in Espionage by Americans: 1947–2007*, Monterey, Calif.: PERSEREC, Technical Report 08-05, 2008; and David Major and Peter C. Oleson, "Espionage in America," in Peter C. Oleson, ed., *AFIO's Guide to the Study of Intelligence*, Falls Church, Va.: Association of Former Intelligence Officers, 2016.

[50] PERSEREC, 2009; Herbig, 2017; and Major and Oleson, 2016.

[51] PERSEREC, 2009, pp. 10, 58–59; and Sulick, 2013, pp. 93–108 and 141–148. For more information on the Walker spy ring, see Pete Earley, *Family of Spies: Inside the John Walker Spy Ring*, New York: Bantam Books, 1988; for more information on the Conrad ring, see Stuart A. Herrington, *Traitors Among Us: Inside the Spy Catcher's World*, New York: Harcourt, 1999.

[52] PERSEREC, 2009, pp. 2–3 and 19–20; elaborated in Sulick, 2013, pp. 189–219. For Ames, see Pete Earley, *Confessions of a Spy: The Real Story of Aldrich Ames*, New York: Putnam, 1997. For Hanssen, see David Wise, *Spy: The Inside Story of How the FBI's Robert Hanssen Betrayed America*, New York: Random House, 2003. For the Russian perspective, see Victor Cherkashin with Gregory Feifer, *Spy Handler: The True Story of the Man Who Recruited Robert Hanssen and Aldrich Ames*, New York: Basic Books, 2004.

[53] James B. Bruce and Michael Bennett, "Foreign Denial and Deception: Analytic Imperatives," in Roger Z. George and James B. Bruce, eds., *Analyzing Intelligence: National Security Practitioners' Perspectives*, 2nd ed., Washington, D.C.: Georgetown University Press, 2014, pp. 197–214.

[54] George Tenet, testimony before the House Permanent Select Committee on Intelligence, "The Impact of Unauthorized Disclosures on Intelligence," November 3, 1999.

[55] Director of the National Counterterrorism Center Matt Olsen's comments were made at the American Political Science Association meeting, Washington, D.C., August 28, 2014. See also Peter C. Oleson, "Assessing Edward Snowden—Whistleblower, Traitor, or Spy?" *The Intelligencer*, Vol. 21, No. 2, Spring/Summer 2015, pp. 15–24.

[56] Ari Fleischer, White House press statement, June 20, 2002.

[57] John Rizzo, former CIA acting general counsel, in *Company Man: Thirty Years of Controversy and Crisis in the CIA*, New York: Scribner, 2014, pp. 148–151. The author of the compromising article was Tim Weiner.

[58] Bruce, 2003, pp. 40–43. For an Indian account of how India used its newfound knowledge of U.S. imagery collection to develop countermeasures, see Raj Chengappa, *Weapons of Peace: The Secret Story of India's Quest to Be a Nuclear Power*, New Delhi: Harper Collins India, 2000, pp. 403, 413–414, 419–420, and 425–428.

[59] Bruce and Jameson, 2013, p. 14; see especially Ross, 2011; and Abel, 1987.

[60] Much of the Snowden controversy, for example, highlights the whistleblower defense, a pillar of the Snowden narrative. The Obama administration refuted that claim; see Nick Gass, "White House: Snowden 'Is Not a Whistleblower,'" *Politico*, September 14, 2016. As of August 23, 2018: https://www.politico.com/story/2016/09/edward-snowden-not-whistleblower-earnest-228163

[61] W. George Jameson, "Holding Leakers Accountable: Considering a Comprehensive Leaks Approach," in Rosenzweig, McNulty, and Shearer, 2014, pp. 213–219.

[62] Sharon LaFraniere, "Math Behind the Leak Crackdown: 153 Cases, 4 Years, 0 Indictments," *New York Times*, July 20, 2013. FBI contractor Shamai Leibowitz, the subject of the first prosecution for leaking to the press during the Obama presidency, was indicted in December 2009. See also Bruce and Jameson, 2013, pp. 10–13.

[63] Stephen P. Mulligan and Jennifer K. Elsea, *Criminal Prohibitions on Leaks and Other Disclosures of Classified Defense Information*, Washington, D.C.: Congressional Research Service, CRS Report R-41404, March 7, 2017, pp. 19–24. The prosecuted leakers include Shamai Leibowitz, Thomas Drake, Jeffrey Sterling, Stephen Jim-Woo Kim, Bradley (now Chelsea) Manning, John Kiriakou, and Donald Sachtelben.

[64] See Eric E. Ballou and Kyle E. McSlarrow, "Plugging the Leak: A Case for Legislative Resolution of the Conflict Between Demands of Secrecy and the Need for an Open Government," *Virginia Law Review*, June 1985, pp. 801–868; and Harold Edgar and Benno C. Schmidt, "The Espionage Statues and the Publication of Defense Information," *Columbia Law Review*, Vol. 73, No. 5, May 1973, pp. 929–1087. For a brief summary update of federal law on press leaks, see Congressional Research Service Reports and Analysis, *The Law and Leaks to the Press: Legal Sidebar*, Washington, D.C., February 22, 2017.

[65] John Ashcroft, letter to the Speaker of the House of Representatives, October 15, 2002. As of August 23, 2018: https://fas.org/sgp/othergov/dojleaks.html

[66] See Jameson in Rosenzweig, McNulty, and Shearer, 2014.

[67] Based on an examination of data over a three-decade period (preceding the Obama policy change in 2009–2013), Gary Ross has concluded that indictments and prosecutions for leaking "have not created a significant deterrent for government employees to discontinue disclosing classified information to the media" (Ross, 2011, p. 17).

[68] See Clapper and Obama's statements in note 1 for characterizations of seriousness.

[69] Herbig, 2017, noted that as many as 86 percent of spies who began their espionage in 2010–2015 used these technologies, showing a steady growth over preceding years, and their use has risen dramatically since 1970–1979, when only 13 percent of spies availed themselves of these technologies (pp. 162–164).

[70] Brian Fung, "5.1 Million Americans Have Security Clearances. That Is More Than the Entire Population of Norway," *Washington Post*, March 24, 2014.

[71] Roughly 100 categories might be a starting point; either a larger or smaller number will have pros and cons. Main topics such as Russia, China, North Korea, Iran, counterterrorism, and counterproliferation could justify four to eight categories each, depending on how broadly or narrowly the bins are defined. The National Intelligence Priorities Framework and the FBI's National Security Threat List, along with the ODNI information management innovations, such as the Library of National Intelligence, will support identifying sensible access categories.

[72] A recent unclassified estimate of 5.1 million (Fung, 2014) may err on the high side by as much as a million.

[73] The President's Review Group in Intelligence and Communications Technologies, *Liberty and Security in a Changing World*, Washington, D.C., December 2013; PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, Washington, D.C., July 2, 2014; and PCLOB, *Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and the Operations of the Foreign Intelligence Surveillance Court*, Washington, D.C., January 23, 2014.

[74] ODNI, "Principles of Intelligence Transparency for the Intelligence Community," webpage, undated.

[75] "Statistical Transparency Report Regarding the Use of National Security Authorities for Calendar Year 2016," *Office of the Director of National Intelligence—IC on the Record*, Tumblr post, undated. As of August 23, 2018: http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2016

[76] Interviews with multiple current and former U.S. government officials, April–May 2016; and observations from the joint RAND Corporation/American Bar Association workshop, June 9, 2016.

[77] Interview with IC official, April 26, 2016.

[78] Interview with IC official, May 20, 2016.

[79] Observation from the joint RAND Corporation/American Bar Association workshop, June 9, 2016.

[80] Interview with IC official, May 20, 2016.

[81] Interview with U.S. government records management official, May 23, 2016.

[82] Interviews with IC officials, April 26, 2016, and May 20, 2016.

[83] Interview with IC official, April 26, 2016.

[84] Observation from the joint RAND Corporation/American Bar Association workshop, June 9, 2016.

[85] Interview with IC official, April 26, 2016.

[86] Interview with U.S. government records management official, May 23, 2016.

[87] Interview with U.S. government records management official, May 23, 2016.

[88] Interview with former IC official, May 25, 2016.

[89] Observations from the joint RAND Corporation/American Bar Association workshop, June 9, 2016.

[90] Observations from the joint RAND Corporation/American Bar Association workshop, June 9, 2016.

[91] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005, p. 381.

[92] Hou Zhongwen and Wang Zongxiao, *Sources and Methods of Obtaining National Defense Science and Technology Intelligence*, Beijing: Kexue Jishu Wenxuan Publishing Company, 1991. Discussed in William C. Hannas, James Mulvenon, and Anna Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*, New York: Routledge, 2013; reviewed by Arturo Munoz in *Studies in Intelligence*, Vol. 59, No. 4, 2015.

[93] See Public Interest Declassification Board, *Setting Priorities: An Essential Step in Transforming Classification*, Washington, D.C., December 2014.

[94] We are indebted to Steven Aftergood for this innovative suggestion in correspondence of June 21, 2016.

[95] The gathering of interview data and workshop deliberations target the most-important views relevant to this study. Kuhn has emphasized the importance of focusing on the paradigm's practitioners: "Any study of paradigm-directed or paradigm-shattering research must begin by locating the responsible group or groups" (Kuhn, 1996, p. 180).

[96] See H. R. Bernard, A. Wutich, and G. W. Ryan, *Analyzing Qualitative Data: Systematic Approaches*, 2nd ed., Thousand Oaks, Calif.: Sage Publications, 2016, Chapter 3.

[97] A. Strauss and J. Corbin, *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*, Thousand Oaks, Calif.: Sage Publications, 1990.

About the Authors

James B. Bruce is an adjunct researcher and former senior political scientist at the RAND Corporation, a retired senior executive officer at the CIA, and an adjunct professor at Georgetown and Florida Atlantic Universities. He served in the National Intelligence Council as deputy national intelligence officer for science and technology and held management positions in the CIA's Directorates of Analysis and Operations. He has published on aspects of secrecy in *Studies in Intelligence*, the *American Intelligence Journal*, anthologies, RAND products, and government studies.

Sina Beaghley is acting associate director for the Cyber and Intelligence Policy Center and a senior international/defense policy researcher at the RAND Corporation, where she focuses some of her research on secrecy and transparency, background investigation and security clearance reforms, and surveillance policy. Before coming to RAND, she served as a member of the White House Disclosures Task Force and as director for intelligence and information security on the National Security Council staff, where she coordinated the U.S. government response to the 2013–2014 unauthorized disclosures related to the National Security Agency.

W. George Jameson is an adjunct at the RAND Corporation; a retired senior official at the CIA; an attorney; a consultant; and the cofounder of the Council on Intelligence Issues, a nonprofit that educates the public on intelligence and national security. His expertise from more than 40 years of government and private-sector experience spans a wide array of national security–related legal, policy, and operational matters, including secrecy, declassification, privacy, counterintelligence, covert action, and intelligence reform.

About This Perspective

This Perspective summarizes our examination of the adequacy of the present system for governing secrecy in U.S. national security information. We conducted an extensive literature review; interviewed 25 senior U.S. government officials and other experts and stakeholders; and benefited from insightful commentary offered at a one-day, 40-person workshop convened in partnership with the American Bar Association, "Assessing the Secrecy Paradigm for the Future Information Environment." Drawing from these interviews, workshop data, and literature, this Perspective analyzes key factors that drive how well or how poorly secrecy works—and why.

Adapting Thomas Kuhn's use of "paradigm" for its conceptual framework, we examine the principal elements of the secrecy paradigm (the structure, culture, rules, and technologies of conducting secrecy) and its processes (the classification of information, how it is safeguarded, and how it becomes available to the public). Together, the way these elements and processes perform and interact with each other determines the overall performance of the secrecy paradigm. We evaluate this performance and, where it is found wanting, offer recommendations to improve it. Fully implemented, the recommendations would constitute a paradigm shift that would greatly improve both government secrecy and transparency.

We thank our RAND Corporation colleagues Brian Gordon and Jenny Oberholtzer for their significant contributions and Gery Ryan and Aaron Frank for their early support of the project. Jamie Baker, Harvey Rishikof, and Holly McMahon of the American Bar Association's Standing Committee on Law and National Security joined with RAND in June 2016 to cosponsor the secrecy workshop, an important input to this study. Stephen Cambone and Martin Faga made especially valuable comments on earlier drafts. Bill Geiger, Ed Kaufhold, Harry Cooper, and Roy Godson also contributed important ideas. We are deeply grateful to our anonymous interviewees and the workshop participants for their thoughtful observations. Of course, we remain fully responsible for any errors of omission or commission. Betsy Kammer cheerfully managed administrative challenges throughout, and Sunny Bhatt's exceptional support of the RAND/American Bar Association workshop proved essential to its success. Finally, we thank RAND's Gritton Award Committee for selecting and funding this project among many worthy proposals for the Fiscal Year 2016 Gene Gritton Award. We hope their confidence is rewarded with the results presented here.

To permit the widest availability of the study findings and recommendations, we used only unclassified information. This study should be of interest to anyone in the U.S. government with responsibility for formulating or implementing policies affecting classified information or its management and to others with interest in the policies and practices that define and regulate secrecy and transparency in government.

$24.00

ISBN-10 1-9774-0110-4
ISBN-13 978-1-9774-0110-6

52400

9 781977 401106

PE-305-OSD