"National Security" Information and the Freedom of Information Act

Christina E. Wells
University of Missouri School of Law, wellsc@missouri.edu

Follow this and additional works at: https://scholarship.law.missouri.edu/facpubs
Part of the Administrative Law Commons, and the National Security Law Commons

Recommended Citation
Available at: https://scholarship.law.missouri.edu/facpubs/847

This Article is brought to you for free and open access by the Faculty Scholarship at University of Missouri School of Law Scholarship Repository. It has been accepted for inclusion in Faculty Publications by an authorized administrator of University of Missouri School of Law Scholarship Repository. For more information, please contact bassettcw@missouri.edu.
"NATIONAL SECURITY" INFORMATION AND THE FREEDOM OF INFORMATION ACT

CHRISTINA E. WELLS*

TABLE OF CONTENTS

Introduction ................................................................................................................. 1195
I. National Security, Classified Information and FOIA Exemption I .................................. 1198
   A. Secrecy and Classified Information—Background and History .................................... 1198
   B. Judicial Review of FOIA Exemption (b)(1) Claims .................................................. 1205
II. Secrecy Beyond Classified Information and FOIA .................................................. 1208
   A. "Sensitive But Unclassified" Information ................................................................. 1209
   B. The Critical Infrastructure Exemption ................................................................ 1213
III. Potential FOIA Amendments Related to National Security Information ................... 1217
Conclusion .................................................................................................................. 1221

INTRODUCTION

Secrecy regarding national security information is a widely accepted phenomenon. As one observer noted:

[A] government must sometimes stringently control certain information that (1) gives the nation a significant advantage over adversaries or (2) prevents adversaries from having an advantage that could significantly damage the nation. . . . In wartime, when a nation's survival is at stake, the reasons for secrecy are most apparent, the secrecy

* Enoch N. Crowder Professor of Law, University of Missouri-Columbia School of Law. Special thanks to James O'Reilly and William Anderson for their thoughtful comments on the earlier versions of this paper. Sarah Baron provided valuable research assistance.

1195
restrictions imposed by government are most widespread, and acceptance of those restrictions by the citizens is broadest.¹

Throughout history, however, such secrecy has proved problematic. Although officials often have credible and legitimate reasons to keep national security information secret, government secrecy initiatives have invariably expanded to encompass information beyond their initial rationale.

Over time, we have come to realize the very real problems associated with excessive government secrecy. In 1966, Congress enacted the Freedom of Information Act² (FOIA) to ensure greater public access to government information. Recognizing, however, that some secrecy is necessary to protect national security, FOIA currently exempts from disclosure “properly classified” information “specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy” (hereinafter “the (b)(1) exemption”).³ FOIA’s reference to “properly classified” information was an attempt to limit secrecy to information legitimately related to national security. Nevertheless, the statute left intact the existing classification process—one that many critics point to as a cause of excessive secrecy. This fact, combined with judicial reluctance to question executive officials invocation of the (b)(1) exemption, has rendered FOIA only marginally effective in battling government withholding of information in the name of national security.

Furthermore, reliance on the national security rationale has proved irresistible to legislative and executive officials who use it to justify withholding beyond FOIA’s exemption for classified information. Recent Bush Administration actions aptly exemplify this phenomenon.⁴ In addition to relaxing classification criteria after the September 11th terrorist attacks,⁵ the Bush Administration encouraged officials to withhold “sensitive but unclassified information,” which arguably should be disclosed under FOIA.⁶ The administration further lobbied heavily for the

---

⁴. All executive administrations have been subject to the creep of secrecy. I focus primarily on the Bush Administration because of its currency, because secrecy has been an integral aspect of its operations, and because many of its attempts at secrecy have been formalized in law.
⁵. See Exec. Order No. 13,292, 3 C.F.R. 196 (2003) (outlining the classification standards, authority, categories, and duration by which information may be kept in confidence by the government).
⁶. See Attorney General John Ashcroft, Memorandum for All Heads of Federal

While there may be legitimate national security interests associated with shielding "sensitive but unclassified" and "critical infrastructure" information from public disclosure, the Bush Administration’s actions are problematic. First, statutes and regulations provide no uniform definition of "sensitive but unclassified" information, a term that initially was not meant to apply to disclosure issues.\footnote{See infra notes 71-74 and accompanying text.} Combined with the Bush Administration’s invocation of the national security rationale, this may cause excessive withholding of information. Second, the "critical infrastructure" exemption from FOIA is overly broad, does not adequately define the information to be withheld, and attaches criminal penalties to disclosure, which also may lead to excessive withholding of information.

Secrecy with respect to national security is important, but the natural tendency of bureaucrats to rely on it—understandably exacerbated in times of crisis—threatens to engulf FOIA’s purpose. Historically, secrecy has continued well beyond identifiable crises, becoming entrenched in even routine matters. The fact that government officials believe the country has subsisted in a constantly threatened state for much of the last 50 years due to the Cold War and terrorism\footnote{See generally Jules Lobel, \textit{Emergency Power and the Decline of Liberalism}, 98 YALE L.J. 1385, 1400-04 (1989) (discussing America’s evolution to a “perpetual state of emergency” in the 20th century due to the changing character of warfare).} suggests that executive officials will continue to invoke the national security rationale to justify even greater withholding of government information.

To counteract the government's predictable creep toward excessive secrecy, Congress should amend FOIA. Although there are many possible avenues one could take, this Article suggests three broad categories of changes. First, Congress should codify an exemption for national security information in a single statute. Consolidation of national security information within one exemption would supplant the current patchwork approach and create an overarching, uniform framework to assess the...
validity of government exemption claims. Providing a tone of openness and clearer guidelines for government officials responsible for secrecy decisions may discourage overzealous classification. Second, Congress should explicitly define the parameters of various exemptions in legislation. Currently, the withholding of information is primarily governed by executive order or a patchwork of statutes and regulations, causing a lack of continuity and creating confusion. Precise legislative definitions and standards would potentially limit some unwarranted executive actions and provide greater clarity. Finally, Congress should require in camera judicial review of documents withheld in the name of national security. Too often judges deferentially review challenges to executive withholding. Explicit congressional requirement of in camera review would encourage judges to scrutinize more carefully officials’ claims and avoid potential separation of powers concerns.

I. NATIONAL SECURITY, CLASSIFIED INFORMATION AND FOIA EXEMPTION I

A. Secrecy and Classified Information—Background and History

Classification of national security information (i.e., the determination that certain government information relevant to national defense or foreign relations should be available only to a few privileged officials) is a primary mechanism of secrecy in government, especially as it relates to public access to knowledge. Government secrecy is, of course, not limited to the classification system. Government officials may, for example, maintain secrecy regarding national security information by asserting executive privilege in response to lawsuits or congressional requests for information, or by closing certain administrative hearings, such as immigration hearings. As the primary mechanism for controlling national security information, however, the classification scheme is one of the “pillars” of government secrecy and generally sets the tone regarding secrecy. It is also the only mechanism of secrecy regarding national security directly governed by FOIA. In discussing whether Congress

10. See Laurence H. Tribe, American Constitutional Law § 4-15, at 769-71 (3d ed. 2000) (explaining that presidential invocation of executive privilege in the name of military or diplomatic objectives has existed since the presidency of George Washington).

11. See N. Jersey Media Group, Inc. v. Ashcroft, 308 F.3d 198 (3d Cir. 2003) (holding “newspapers did not have a First Amendment right of access to deportation proceedings that were determined by the Attorney General to present significant national security concerns”).

should amend FOIA, this Article focuses on the classification system, its relationship to other national security information, and its potential for abuse.

The classification process within the United States has been and remains governed almost entirely by executive order. Such orders typically define the type of information that can be classified; the levels of classification; who has classification authority; and the length of time material can be classified. President Bush’s current order, for example, states that information can be classified only if it concerns:

(1) military plans, operations, and weapons systems,
(2) foreign government information,
(3) intelligence activities, sources or methods,
(4) foreign relations or foreign activities of the U.S.,
(5) scientific, technological, or economic matters relating to national security,
(6) government programs for safeguarding nuclear materials, and weapons of mass destruction.

It also prohibits government officials from classifying certain material, such as basic scientific research. The order further provides that information may be classified at three levels: (1) top secret; (2) secret; and (3) confidential—terms that are defined as information “the unauthorized disclosure of which reasonably could be expected to cause,” respectively, “exceptionally grave damage,” “serious damage,” or “damage,” to national security.

President Bush’s order, like those of his predecessors, is the product of a process that, although reasonably well entrenched, has significant problems. Because the classification scheme is defined by executive order, there is no legislative oversight, leaving executive officials with broad discretion to determine the information to be classified, the duration of classification, and other important details of the secrecy process. As discussed below, executive officials have historically wielded this power expansively, withholding information only remotely pertaining to national security.

13. Occasionally, a statute provides classification criteria in limited circumstances. The Atomic Energy Act, for example, provides legislative parameters with respect to classification of information relating to nuclear weapons. 42 U.S.C. §§ 2161-2166, 2271-2284 (2000). In general, however, most classifications are governed by executive order.
15. Id. at § 1.7(b).
16. Id. at § 1.2. Among other things, Bush’s order also limits the duration of classification to either 10 or 25 years depending upon the sensitivity of the information, although such terms can be extended, and provides for automatic declassification of certain documents 25 years and older. Id. §§ 1.5, 3.3.
Originally the classification system, a creation of the military establishment, was narrowly limited to safeguarding military information. With the advent of nuclear weapons and the Cold War, however, government officials began to broadly interpret the concept of national security. As the United States became a superpower, "[e]very challenge to the United States hegemony anywhere in the world began to be perceived as a threat to national security." This broad notion of threat expanded our defensive frontiers from protection against concrete, physical threats against the country's borders to include potential threats to the country's interests posed by worldwide events. Further, the term "national security" came to implicate threats to "the entire resources of the nation—not only its [military and] intelligence apparatus, but its scientific, industrial, and economic capabilities."

This wide-reaching notion of national security affected executive branch classification of information. In 1951, President Truman's executive order expanded government secrecy by extending the classification system to include civilian agencies and allowed classification of all information "the safeguarding of which is necessary in the interest of national security," a category far broader than previous orders pertaining to "national defense." Although subsequent classification systems have varied somewhat with administrations, most have followed Truman's lead,

---

17. See Harold Relyea, The Presidency and the People's Right to Know, in THE PRESIDENCY AND INFORMATION POLICY 1, 12-20 (Harold Relyea et al. eds., 1981) (finding that "[t]he first system for the protection of national defense documents and papers" included "submarine mine projects and land defense plans); see also Williams S. Moorhead, Operation and Reform of the Classification System in the United States, in SECRECY AND FOREIGN POLICY 87, 94 (Thomas M. Franck & Edward Weisband eds., 1974) (emphasizing that throughout the early period of classification procedures, such rules applied to "safeguarding military secrets" and did not extend to non-military agencies).

18. Lobel, supra note 9, at 1400.


20. See Exec. Order No. 10,290, 3 C.F.R. 790 (1949-53); see also Quist, supra note 1, at Ch. 3 (comparing Truman order with previous classification systems).

21. Presidents Eisenhower and Kennedy, for example, attempted to narrow Truman's order. See Quist, supra note 1, at Ch. 3. Presidents Carter and Clinton also tried to rein in secrecy while Presidents Nixon and Reagan and the current President Bush signed executive orders vastly expanding the government's ability to classify information. For discussions of various administration's approaches to classification, see Relyea, supra note 17, at 24-26 (describing Carter's pledge of "maximum security declassification); Moorhead, supra note 17, at 102-05; Morton H. Halperin, The President and National Security Information, in THE PRESIDENCY AND INFORMATION POLICY (Harold Relyea et al. eds., 1981), supra note 17, at 68-69 (describing Carter's order and its affect on FOIA); and HERBERT N. FERSTERL, FREEDOM OF INFORMATION AND THE RIGHT TO KNOW 51-57 (Greenwood Press 1999) (discussing Reagan Executive Order 12,356 which "eliminated the need for government agencies to consider the public's right to know when deciding whether to release information").
allowing classification by civilian agencies and relying on the amorphous "national security" standard. 22

Since the Truman era, most commentators agree that executive officials have been too secretive regarding national security information. During the 1950s, several governmental commissions concluded that overclassification was a problem. 23 The Commission on Government Security, for example, concluded that too many government employees were classifying information in a manner that impeded scientific and technological research and, consequently, actually posed a threat to national security. 24 Investigators of excessive secrecy during the 1970s came to similar conclusions, as testimony from government officials estimated that 90 to 99.5% of information in some departments was inappropriately classified. 25 While problems with excessive secrecy improved somewhat during the Clinton era, 26 a 1997 commission found that some experts still estimated that only 10% of classification actions involved "'legitimate protection of secrets.'" 27

Most recently, the Bush administration appears to have embraced secrecy regarding national security information. Classification of information in the Bush administration increased fourteen percent from


23. See generally Availability of Information from Federal Departments and Agencies: Hearings Before A House Subcommittee of the Committee of Government Operations, 84th Cong. 85th Cong. (1956-58); REPORT OF THE COMMISSION ON GOVERNMENT SECURITY (1957) [hereinafter WRIGHT COMMISSION REPORT] (discussing overclassification problems under Presidents Truman and Eisenhower, identifying sources of overclassification, and recommending changes to the classification system); see also, Moorhead, supra note 17, at 96 (discussing the Wright Commission and its recommendation to reduce the number of government employees authorized to classify documents).

24. WRIGHT COMMISSION REPORT, supra note 23, at 174-76.

25. U.S. GOVERNMENT INFORMATION POLICIES AND PRACTICES—THE PENTAGON PAPERS: HEARINGS BEFORE A SUBCOMM. OF THE HOUSE COMM. ON GOV'T OPERATIONS, 92d Cong., pt. 1, 12 (1971) (citing testimony of former U.N. Ambassador Arthur Goldberg estimating that 90% of the classified documents with which he had been involved were wrongly classified or should have been declassified almost immediately); see also id. at 97 (citing statement of William Florence, retired Air Force security analyst, to the effect that 99.5% of the information within the defense department could be declassified without endangering national security).

26. See Thomas S. Blanton, National Security and Open Government in the United States: Beyond the Balancing Test, in NATIONAL SECURITY AND OPEN GOVERNMENT: STRIKING THE RIGHT BALANCE 33, 52-54 (2003), at http://www.maxwell.syr.edu/campbell/opengov/NSOG.pdf (last visited June 8, 2004) (referring to President Clinton's "release of more than forty million pages of secret documents" and "ordering sunsets and specific justifications on each secret" a process which included "automatic declassification").

27. See MOYNIHAN COMMISSION, supra note 12, at 36 (quoting National Security Council Executive Secretary Rodney B. McDaniel).
2001 to 2002. In 2003, Bush administration officials classified over 14 million documents, an increase of 14% over the previous year. A Bush administration official has acknowledged that “up to half of what the government now classifies needn’t be.” This increase in classification occurred while the Bush administration operated under President Clinton’s order. President Bush’s new order, issued March 25, 2003, likely will encourage even greater secrecy. Although the new order retains many characteristics of the more liberal Clinton order, it encourages secrecy by increasing the length of time material can be classified, lowering the standard under which material can be exempted from declassification, making it easier to reclassify material, and removing a Clinton era presumption that when there exists doubt regarding the appropriateness of classification, the issue should be resolved in favor of openness. Such changes, while seemingly minor, promote greater secrecy by “changing the ‘default’ setting from ‘do not classify’ to ‘classify.’”

Given human nature, over-classification and the tilt toward secrecy is an understandable phenomenon. All executive orders instruct classifiers to gauge the type of threat information poses to national security when determining whether and at what level to classify information. Given the current understanding of the term “national security” as encompassing all potential threats to United States interests, the classification process does not involve identification of concrete threats but “is a prophylactic concept, concerned with potential dangers—with ‘intangibles, uncertainties and probabilities.’” In light of such uncertainty, executive officials have every incentive to read a classification charge expansively. In fact, psychological studies suggest that executives will err on the side of safety when something as important as national security is at stake. This may be

29. See id. at 18-20.
33. National Security and FOIA, supra note 19, at 411.
true regardless of the classification scheme in place, but vesting the executive with unfettered discretion to define the meaning of "national security" and to set the tone regarding secrecy clearly exacerbates this problem as executive officials, lacking accountability to independent authorities, have no incentive to exercise diligence in their decisions. Allowing the executive to change schemes at will causes further confusion among lifetime bureaucrats, leaving them without guidance when making difficult classification assessments.

In addition to encouraging simple errors in classification, the current classification scheme facilitates over-classification arising from other motives. Bureaucrats tend toward secrecy because it allows them to maintain their power.\textsuperscript{35} History is rife with examples of executive officials classifying information in order to avoid embarrassment, protect political agendas, or hide affirmative government misconduct. Soon after World War II, for example, the government secretly participated in the forced repatriation of anti-communist Russians, refusing over 20 years later to declassify its files on the subject.\textsuperscript{36} In the 1960s, executive officials maintained secrecy regarding the government's policies in Vietnam\textsuperscript{37} and its war in Cambodia\textsuperscript{38} to facilitate public support and prevent revelations of embarrassing failures. Similarly, the Nixon Administration hid its secret support of Pakistan during the 1971 India-Pakistan War to avoid upsetting the American public.\textsuperscript{39}

The current administration has also been accused of classifying information with these motives in mind. Members of the independent commission examining the September 11th terrorist attacks, for example, have publicly expressed frustration with the administration's refusal to

\begin{itemize}
  \item \textsuperscript{35} Max Weber, From Max Weber: Essays in Sociology 233-34 (H.H. Gerth & C. Wright Mills trans. 1958) ("Every bureaucracy seeks to increase the superiority of the professionally informed by keeping their knowledge and intentions secret.").
  \item \textsuperscript{37} Incidents and information initially kept secret but eventually coming to light included the My Lai massacre, the authorization of bombing strikes on "off-limits" targets, and the creation of the Pentagon Papers, a history of government decision-making regarding the Vietnam War. Moorhead, supra note 17, at 89; see also Developments in the Law—The National Security Interest and Civil Liberties, 85 Harv. L. Rev. 1330, 1197-98 (1972) ("The publication of the top secret ‘Pentagon Papers’ has intensified the debate over the proper role for secrecy in the conduct of defense and foreign affairs").
  \item \textsuperscript{38} The Nixon administration publicly claimed that it had not bombed Cambodia despite 14 months of air raids. It further falsified information to that effect in classified reports to Congress. Arthur Schlesinger, The Imperial Presidency 356-57 (1973).
  \item \textsuperscript{39} The Nixon Administration publicly proclaimed neutrality but secretly supported Pakistan. Id. at 357.
\end{itemize}
share classified information with them, claiming that much of the material reviewed was wrongly classified and that the administration was withholding information for political reasons. Some congressional members participating in the congressional inquiry regarding September 11th also claim that the administration classified portions of its report regarding potential foreign government involvement with the September 11th terrorists for political reasons. In light of recent revelations regarding abuse of prisoners at the Abu Ghraib detention center in Iraq, and the Bush Administration’s torture memoranda, the American Civil Liberties Union (ACLU) recently accused the Bush administration of unreasonably withholding information regarding torture of detainees in response to FOIA requests last year. Finally, critics charge that the administration has selectively declassified information supporting the war in Iraq while keeping classified material that would have argued against the war.

Such scandals attest to at least one of the costs of excessive secrecy—lack of political accountability. Excessive secrecy also leads to poor decision-making by insulating those responsible for decisions from scrutiny, ultimately impeding scientific and technological research by

---


42. See ACLU, U.S. Illegally Withheld Records on Abuses at Abu Ghraib and Elsewhere (June 2, 2004), available at www.aclu.org/news/NewsPrint.cfm?ID=15885&c=206 (last visited June 10, 2004). A federal district court eventually ordered the government to produce or identify all documents responsive to the ACLU’s request, noting that the “glacial pace at which defendant agencies have been responding to plaintiffs’ requests shows an indifference to the commands of FOIA, and fails to afford accountability of government that the act requires.” ACLU v. Dep’t of Defense, 2004 WL 2050921 at *3 (S.D.N.Y. 2004).


44. See MOYNIHAN COMMISSION, supra note 12, at 7 (“Secrecy has the potential to undermine well-informed judgment by limiting the opportunity for input, review, and
barring the sharing of information.\textsuperscript{45} Finally, it detracts from the purposes of keeping information confidential by diluting the value of legitimately secret information.\textsuperscript{46}

B. Judicial Review of FOIA Exemption (b)(1) Claims

In 1966, Congress, recognizing problems with excessive secrecy, enacted FOIA.\textsuperscript{47} The statute was designed to provide the public with a legal right of access to government information, operating on a presumption of “full agency disclosure unless information is exempted under clearly delineated statutory language.”\textsuperscript{48} The Act listed nine exemptions upon which the government could rely in withholding information but also provided de novo judicial review of all claims of exemption.\textsuperscript{49} As in the current statute, the original statute provided an exemption for national security, allowing withholding of information “specifically required by Executive order to be kept secret in the interest of the national defense or foreign policy.”\textsuperscript{50}

Initially, lower courts deferred to executive invocation of the (b)(1) exemption, allowing government officials to resist disclosure of criticism, thus allowing individuals and groups to avoid the type of scrutiny that might challenge long-accepted beliefs and ways of thinking.”). Psychologists have noted this phenomenon in government decisionmaking. \textit{See generally} IRVING JANIS, GROUPTHINK: PSYCHOLOGICAL STUDIES OF POLICY DECISIONS AND FIASCOS (1982) (elaborating on the Groupthink phenomenon found in government decision-making in times of crisis).

45. \textit{See MOYNIHAN COMMISSION, supra note 12, at 8 (“[T]he classification of technical information impedes its flow within our own system, and may easily do far more harm than good by stifling critical discussion and review or by engendering frustration.”)(quoting Report of the Defense Science Board Task Force on Secrecy 9 (1970)); see also Executive Privilege, Secrecy in Government, Freedom of Information, Hearings before the Subcommittee on Intergovernmental Relations of the Committee on Government Operations and the Subcommittees on Separation of Powers and Administrative Practice and Procedure of the Committee on the Judiciary, 93d Cong., 302 (1973) (statement of Dr. Earl Callen) (“Secrecy is inimical to science.”) [hereinafter Executive Privilege Hearings].

46. \textit{See N.Y. Times Co. v. United States, 403 U.S. 713, 729 (1971) (Stewart, J., concurring) (“[W]hen everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion.”).}


48. S. REP. NO. 89-813, at 3 (1965). Congress was responding to problems with Section 3 of the Administrative Procedure Act (APA), which allowed executive officials to withhold information to protect “any function of the United States requiring secrecy in the public interest.” Act of June 11, 1946, ch. 324, § 3, 60 Stat. 238. Congress believed this provision to be inadequate because it precluded judicial review by allowing “any government official... [t]o withhold almost anything from any citizen under the vague standards or, more precisely, lack of standards in section 3.” \textit{Id.} at 5.


Furthermore, in *EPA v. Mink*, the Supreme Court interpreted the original (b)(1) exemption as allowing judges to review only the procedural propriety of the classification and not whether a government classification decision was substantively proper under the relevant executive order. In 1974, Congress amended the (b)(1) exemption by adding the requirement that national security information in fact be "properly classified pursuant to ... Executive Order." Congress further provided courts with discretion to review documents in camera and to require release of non-exempted portions of documents if reasonably segregable. The conference report accompanying the amendments made clear that Congress intended to overrule *Mink* and provide effective judicial review of executive branch classification decisions.

While strengthening judicial review of the (b)(1) exemption, the conference report also stated:

> [T]he conferees recognize that the Executive departments responsible for national defense and foreign policy matters have unique insights into what adverse affects might occur as a result of public disclosure of a particular classified record. Accordingly, the conferees expect that Federal courts, in making de novo determinations in section 552(b)(1) cases under the Freedom of Information law, will accord substantial weight to an agency's affidavit concerning the details of the classified status of the disputed record.

Apparently inserted as an attempt to appease President Ford, who threatened to veto new provisions over separation of powers concerns, the conference statement sent mixed signals regarding courts roles in reviewing (b)(1) exemptions. As a result, courts reviewing (b)(1) exemption challenges still give great deference to executive classification decisions.

Most courts at least purport to exercise de novo review in accordance with the 1974 amendments, generally adhering to the description set forth in *Ray v. Turner*:

1. The government has the burden of establishing an exemption.
2. The court must make a *de novo* determination. (3) In doing this, it must first accord substantial weight to an agency's affidavit concerning the details of the classified status of the disputed

51. *See generally* Epstein v. Resor, 421 F.2d 930, 933 (9th Cir. 1970) ("[W]hat is desirable in the interest of national defense and foreign policy is not the sort of question that courts are designed to deal with.").
52. 410 U.S. 73, 82 (1973).
54. *Id.* § 552(a)(4)(B).
56. *Id.* at 12.
57. President Ford did veto the amendments, which Congress eventually overrode. SOURCE BOOK, *supra* note 36, at 403-85.
58. 587 F.2d 1187 (D.C. Cir. 1978).
(4) Whether and how to conduct an in camera examination of the documents rests in the sound discretion of the court, in national security cases as in all other cases. [Finally, if]... exemption is claimed on the basis of national security the District Court must, of course, be satisfied that proper procedures have been followed, and that by its sufficient description the contested document logically falls into the category of the exemption indicated.59

The courts' interpretation of this standard, however, can vary dramatically.

Much of the difference comes about with respect to court treatment of government affidavits supporting its claims of exemption. Typically, this involves a description of the documents withheld, how they fall into a particular category of classified information (e.g., military plans), a defense of their categorization level (e.g., an explanation of how disclosure of information "reasonably could be expected to damage national security" in accordance with its designation as "confidential"), and a discussion showing that proper procedures were followed.60

Some courts exercise reasonably aggressive review of such affidavits, finding the government’s submission inadequate unless it contains detailed and particularized explanations of the classification decision and the possible effects of disclosure.61 Most courts, however, rarely engage in such review, instead holding that the government is entitled to summary judgment if its affidavits describe the information withheld and the justification for withholding it with reasonable specificity, the information logically falls within the claimed exemptions, and there is no evidence on the record to controvert the government’s affidavits or show government bad faith.62 Many of those courts make clear that if the government’s arguments are logical or plausible “the court is not to conduct a detailed inquiry to decide whether it agrees with the agency’s opinions; to do so would violate the principle of affording substantial weight to the expert

59. Id. at 1194-95 (quoting Weissman v. CIA, 565 F.2d 692, 697 (D.C. Cir. 1977)).

60. See supra notes 52-54 and accompanying text (reviewing pertinent exemptions and provisions for judicial review of determinations that particular information is subject to exemption).


opinion of the agency. Many further find that in camera review of the government’s documents is not only unnecessary but also inappropriate if the government’s affidavits meet the above conditions.

Most observers agree that courts are generally deferential to claims of harm to national security, rarely overriding the government’s classification decisions. Although purporting to apply de novo review, they effectively apply something less. Court cases involving the (b)(1) exemption decided after the September 11th terrorist attacks suggest that this deferential trend will continue. Courts have refused to require disclosure of information regarding the implementation of the USA Patriot Act or the reasons underlying one plaintiff’s loss of her security clearance at the INS, noting that “the court should not second-guess an agency’s ‘facially reasonable concerns’ regarding the harm disclosure may cause to national security.”

Further, one court has deferred to national security concerns in reviewing a (b)(7) exemption regarding law enforcement records, despite the fact that such deference is intended for (b)(1) exemptions only.

II. SECRECY BEYOND CLASSIFIED INFORMATION AND FOIA

Secrecy’s creep is not manifested simply in expansive views regarding classification. The government also has sought to keep information secret in the name of national security even though it admittedly does not meet classification standards. “Sensitive but classified” information and “critical infrastructure” information fall into this category. Although government

63. Halperin, 629 F.2d at 148; see, e.g., Hayden v. Nat’l Sec. Agency/Cent. Sec. Serv., 608 F.2d 1381, 1384 (D.C. Cir. 1979) (applying principle of “substantial weight” and deferring to agency expertise); Gardels, 689 F.2d at 1105 (“The test is not whether the court personally agrees with the [agency’s] evaluation of the danger—rather, the issue is whether . . . the Agency’s judgment objectively survives the test of reasonableness, good faith, specificity and plausibility.”); Canning, 848 F. Supp. at 1042 (noting that courts must give “substantial weight” to agency affidavits in light of agency expertise in matters of national defense and foreign policy).

64. See generally Hayden, 608 F.2d at 1387; Canning, 848 F. Supp. at 1042-43.


68. See Ctr. for Nat’l Sec. Studies v. U.S. Dep’t of Justice, 331 F.3d 918, 927 (D.C. Cir. 2003) (“[W]e have consistently deferred to executive affidavits predicting harm to the national security, and have found it unwise to undertake searching judicial review.”).

69. See Alyeska Pipeline Serv. Co. v. EPA, 856 F.2d 309, 315 (D.C. Cir. 1988) (clarifying the D.C. Circuit’s reluctance to “extend any special deference beyond the Exemption 1 context”); see also Wash. Post Co. v. U.S. Dep’t of State, 840 F.2d 26, 33-36 (D.C. Cir. 1988) (reviewing legislative history of exemptions). Some (b)(3) exemptions also receive such deference in classification-related circumstances. See infra notes 93, 109-10 and accompanying text.
secrecy attempts regarding such information preceded September 11th, the Bush Administration’s aggressive actions since that date regarding both “sensitive but unclassified” and “critical infrastructure” information illustrate some of the problems associated with expanding secrecy and FOIA.

A. “Sensitive But Unclassified” Information

The term “sensitive but unclassified” is difficult to characterize as both its definition and purpose have evolved and been subject to inconsistent agency usage. Congress first used the term “sensitive but unclassified” in the Computer Security Act of 1987 (CSA). Designed to provide uniform standards to protect the privacy and security of information in federal government computers, the CSA defined the term “sensitive but unclassified” as:

information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under [5 U.S.C. § 552a], but which has not been specifically authorized under criteria established by an Executive order or Act of Congress to be kept secret in the interest of national defense or foreign policy.

CSA’s purpose was not to prevent public disclosure of all “sensitive but unclassified” information. Rather, Congress was concerned primarily with unauthorized access or use of insecure computer databases by persons who might use the information for fraudulent or abusive purposes. As a result, Congress made clear that:

the designation of information as sensitive under the Computer Security Act is not a determination that the information is not subject to public disclosure nor does such a designation bear on the determination to disclose. Information that requires protection while it is being


72. Id.

transmitted over telecommunications facilities or while it is being stored in a computer may nevertheless be public information under the Freedom of Information Act. . . . 74

Over time, however, agencies have come to use the term "sensitive but unclassified" in a different manner. Some agencies essentially use the definition in the CSA while others use far broader definitions. The Department of Energy, for example, expansively defines "sensitive but unclassified" as: "[i]nformation for which disclosure, loss, misuse, alteration or destruction could adversely affect national security or government interests," defining the latter as including economic, human, financial, industrial, agricultural, technological, law enforcement, confidential, and commercial proprietary information. 75 Others have declared that "sensitive but unclassified" denotes all information exempt under FOIA or the Privacy Act. 76 Most recently, the Department of Homeland Security (DHS) defined such information to include "information not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest." 77 Thus a patchwork of definitions exists, ranging from those narrowly construing the term to those including almost any matter in which the government is involved.

Second, the term "sensitive but unclassified" no longer simply delineates information, the integrity of which must be protected from misuse while in computer databases. Rather, agencies often use it to refer to any document or electronic information that fits their definition. 78 This change in context also reflects a change in thinking regarding the need to protect information. The "sensitive but unclassified" designation apparently no longer involves safeguarding information while in the government's control. It now designates information that is to be generally protected from disclosure. The Department of State, for example, describes its use of the term as an "'administrative control designation' to protect 'documents that do not contain national security information but must be protected from disclosure.'" 79 In short, despite its original definition and context, current

75. See Knezo, supra note 70, at 20-21 (quoting Department of Energy definition).
78. See U.S. Dep't of State, 12 FAM 540 Sensitive But Unclassified Information (1999) [hereinafter 12 FAM 540], at http://www.foia.state.gov/masterdocs/12fam/12m0540.pdf (last visited June 15, 2004) (describing information "which warrants a degree of protection and administrative control that meets the criteria for exemption from public disclosure").
79. U.S. Dep't of State, 5 FAH-1 H-130, Security Requirements 3 (July 1, 2002), at
use of the term "sensitive but unclassified" involves a chaotic scheme of varied, and sometimes conflicting, agency determinations that certain information is to be protected from public disclosure.80

Observers have noted that this treatment of "sensitive but unclassified" information contributes to excessive secrecy by causing overclassification:

[T]here is little oversight of which information is designated as sensitive, and virtually any agency employee can decide which information is to be so regulated . . . . Moreover, the very lack of consistency from one agency to another contributes to confusion about why this information is to be protected and how it is to be handled. These designations sometimes are mistaken for a fourth classification level, causing unclassified information with these markings to be treated like classified information.81

Such classification errors are likely to go uncorrected. As discussed above, executive officials have little incentive to risk administrative penalties imposed for unauthorized disclosure (of which there are often many pertaining to "sensitive but unclassified" information).82 Thus, classification is the easiest and safest route. Furthermore, courts are unlikely to rectify this problem as they frequently defer to government claims regarding the (b)(1) exemption, the context in which claims of overclassification are raised.

Recent Bush Administration actions will likely exacerbate problems of excessive secrecy regarding "sensitive but unclassified" information. In March 2002, White House Chief of Staff Andrew Card issued a memorandum directing agencies to safeguard government information "regarding weapons of mass destruction, as well as other information that could be misused to harm the security of our Nation and the safety of our people."83 A supplemental memorandum written by Laura Kimberly, Acting Director of the Information Security Oversight Office, provided guidance for implementing the Card memorandum, noting that in

http://www.foia.state.gov/masterdocs/05fah01/CH0130.pdf (last visited June 15, 2004);


81. MOYNIHAN COMMISSION, supra note 12, at 29.

82. See generally 12 FAM 540, supra note 78, at 2 ("Unauthorized disclosure of SBU information may result in criminal and/or civil penalties."); DHS Directive, supra note 77, at § 5 (referring to possible administrative and disciplinary action for unauthorized disclosure).

safeguarding "sensitive but unclassified" information, agencies should give "full and careful consideration to all applicable FOIA exemptions" in accordance with an earlier Ashcroft directive encouraging agency officials aggressively to interpret FOIA in favor of withholding information.\footnote{84}

The Bush Administration's actions will encourage excessive secrecy in many ways. Most obviously, the Card and Kimberly memorandums solidify the apparent understanding of the term "sensitive but unclassified" as a designation associated with disclosure issues. Agency personnel operating with this background understanding may be emboldened to freely use the "sensitive but unclassified" designation to justify withholding of information. Furthermore, the Card and Kimberly memoranda encourage such withholding without providing agency personnel with a usable definition of "sensitive but unclassified" information.\footnote{85} The only guidance with respect to the information covered is the Card memorandum's reference to "[g]overnment information regarding weapons of mass destruction, as well as other information that could be misused to harm the security of our nation [or threaten public safety]."\footnote{86} That definition, however, is so broad as to be useless in terms of providing clear guidelines capable of reining in overzealous officials. Rather, that language merely sets a tone encouraging government officials to use their widely varied "sensitive but unclassified" definitions to withhold information under the FOIA. With some government officials estimating that nearly 75 percent of all government-held information is "sensitive but unclassified,"\footnote{87} the effect of such an approach could be substantial.

Courts could, of course, temper abuse of the "sensitive but unclassified" designation by finding that withheld documents do not fall within an existing FOIA exemption. As long as "sensitive but unclassified" withholdings are made in the name of national security, however, there remains a distinct possibility that courts will defer to the government claims and allow information to be withheld even if actually unrelated to national security concerns.\footnote{88}

\footnote{84. See Kimberly Memorandum, \textit{supra} note 6. Specifically, the Kimberly memorandum urged agencies to apply aggressively FOIA's (b)(2) and (b)(4) exemptions regarding, respectively, "internal personnel rules and practices of an agency" and personal and confidential "trade secrets and commercial or financial information." \textit{Id.} (citing 5 U.S.C. § 552(b)(2), (b)(4) (2000)).}
\footnote{85. The OMB is working on a guidance regarding "sensitive but unclassified" information but has yet to issue it. Knezo, \textit{supra} note 70, at 37.}
\footnote{86. Card Memorandum, \textit{supra} note 6.}
\footnote{87. Joint Security Commission Report, \textit{supra} note 79, at 33.}
\footnote{88. See \textit{supra} notes 60-62 and accompanying text.}
B. The Critical Infrastructure Exemption

Just as national security came to be defined more broadly after World War II, in recent years the government also broadened the spectrum of American society responsible for protecting national security. In 1997, the President’s Commission on Critical Infrastructure Protection noted that the nation’s infrastructure (e.g., energy, banking and finance, telecommunications, transportation, vital human services) was at risk from various threats. Noting much of this infrastructure is privately owned, the report concluded that “national defense is no longer the exclusive preserve of government, and economic security is no longer just about business. [Critical infrastructure is] central to our national defense and our economic power, and we must lay the foundations for [its] future security on . . . cooperation between government and the private sector.”

As part of that cooperation, the commission found that increased information sharing between government and private entities was an immediate need. It further noted that, because private industry was reluctant to share information due to liability concerns and fear of losing competitive advantage, Congress should consider enacting a FOIA exemption protecting the shared material as an incentive for information exchange. Such protection would be tantamount to giving the same kind of confidentiality status to private information that classified status gives to government-held information regarding national security.

At the time, Congress did not enact such an exemption. After the September 11th terrorist attacks, however, the Bush Administration lobbied for and received a FOIA exemption in the Homeland Security Act of 2002. The Act allows the DHS to withhold “critical infrastructure information . . . that is voluntarily submitted” to it by private entities “regarding the security of critical infrastructure and protected systems.”

The Act defines critical infrastructure as physical or virtual systems “so vital to the United States that [their] incapacity or destruction would have a

90. Id.
91. Id. at 21.
92. Id. at 27, 31.
93. See O’Reilly, supra note 47, § 13.14 (noting that an exemption for critical infrastructure information created an “almost-classified category”).
debilitating impact on security, national economic security, [or] national public health or safety."\(^9\) It further defines "critical infrastructure information" as information "not customarily in the public domain [that is] related to the security of critical infrastructure or protected systems," including information regarding (1) actual or potential interference via physical or computer-based attack, or other similar conduct that violates law or threatens interstate commerce or public safety; (2) any planned or past assessment, projection, or estimate of vulnerability to interference, including security testing, risk evaluation, risk management planning, or risk audit; or (3) any planned or past operational problem or solution, including repair, recovery, reconstruction, insurance, or continuity related to interference.\(^7\) In addition to providing a FOIA exemption, the Act imposes criminal penalties for unauthorized disclosure of information, provides companies with immunity from civil liability based on such information, and preempts state access laws.\(^8\) As with the 1997 commission, those favoring the FOIA exemption argue that it was necessary to ensure adequate information-sharing critical to protecting the nation's security.\(^9\)

While information-sharing regarding potentially vulnerable targets is a laudable goal, especially in light of the government's past lapses,\(^10\) the new FOIA exemption suffers from significant problems likely to cause excessive secrecy regarding information only tangentially related to national security. The Act's definition of "critical infrastructure" never identifies which systems or industries are critical to the safety of the nation, instead leaving it to the DHS to identify such systems. Further, there is no commonly accepted understanding of the term, with some viewing the

---

issue of critical infrastructure as primarily a cyber systems problem, and others extending the definition to include national monuments, the destruction of which might hurt the nation’s morale. This lack of guidance is exacerbated by the definition of “protected systems” included within the Act’s definition of “critical infrastructure,” which encompasses “any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure.” The potential breadth of the DHS’s definition is staggering. The broad discretion left with the agency is akin to that given the President to identify classified information, suggesting that the “critical infrastructure” exemption could be subject to the same kinds of abuses. That there are criminal penalties attached to disclosure of such information further exacerbates this problem as agency officials have skewed incentives to interpret the exemption broadly to protect themselves.

Further compounding this potential for abuse are other vague definitions. “Critical infrastructure information” for example, is not limited to vulnerabilities regarding such systems but may include repairs, even for routine reasons, to anything qualifying as critical infrastructure. Similarly, the term “voluntarily submitted” includes information submitted “in the absence of [an] agency’s exercise of legal authority to compel access to or submission of such information.” It is unclear whether that

101. The 1997 commission identified transportation, oil and gas production and storage, water supply, emergency services, banking and finance, electrical power, and telecommunications as critical infrastructure. See CRITICAL FOUNDATIONS, supra note 89, at 3-4. However, though discussing physical assets, it clearly focused on cyber security regarding those assets as the primary vulnerability. Id. at 11, 15-19. See also Rena Steinzor, “Democracies Die Behind Closed Doors”: The Homeland Security Act and Corporate Accountability, 12 KAN. J.L. & PUB. POL’Y 641, 642-43 (2003) (stating that possible cyberspace terrorist attacks resulted in proposed legislation authorizing secret consultations).

102. Moteff et al., supra note 70, at 7.


105. For a more thorough discussion, see Steinzor, supra note 101, at 646-47.

definition means that information is voluntarily submitted if the agency has no legal authority to mandate submission or simply that the agency has not exercised its legal authority. If the latter, the exemption’s breadth expands dramatically.

Commentators argue that the exemption’s breadth reveals that it is less about national security than it is about protecting business interests. Inasmuch as executive officials have used the classification system to hide embarrassing and illegal activity, commentators fear businesses will use the critical infrastructure exemption to do essentially the same. To support their qualms, they note that the Bush Administration’s original proposal contained a narrower exemption for information pertaining to infrastructure “vulnerabilities” but that the language subsequently expanded, suggesting that industry lobbying, rather than national security, was the driving issue. They further argue that the civil immunity provision provides industry a strong incentive to interpret the term “critical infrastructure information” broadly in order to hide information. Finally, they argue that the new exemption is unnecessary as current FOIA exemptions—the (b)(2) exemption for agency personnel rules and practices and the (b)(4) exemption for confidential business records—provide the core protections that industry seeks; the new exemption simply encourages abuse.

Overall, the critical infrastructure exemption from FOIA is subject to many of the abuses of secrecy that have run rampant in the national security context. As in other instances, it is unclear whether courts will check these abuses. The “critical infrastructure” exemption is a (b)(3) exemption (i.e., material specifically exempted by statute). Courts have applied (b)(1) deference to (b)(3) exemptions in situations where the information in question relates to national security in essentially the same way as classified information. Because the critical infrastructure exemption is linked closely to “national security” concerns, there is reason to believe that courts will defer to government claims of exemption. Furthermore, to the extent that material withheld under the critical infrastructure exemption overlaps with the (b)(4) exemption on confidential

110. Id. at S1423-4 (statement of Sen. Leahy); see also Stephen Gidiere & Jason Forrester, *Balancing Homeland Security and Freedom of Information*, 16 NAT. RESOURCES & ENV'T 139 (2002). Interestingly, the Kimberly memorandum specifically referenced these two provisions as ways to safeguard critical infrastructure information suggesting that the Bush administration was aware of adequate existing protections prior to lobbying for a new exemption. See Kimberly Memorandum, supra note 6 (detailing FOIA procedures).
business records, courts already defer to certain claims under that exemption.\textsuperscript{112} Reading it in light of national security concerns suggests that courts will be just as, if not more, deferential to the critical infrastructure exemption.

III. POTENTIAL FOIA AMENDMENTS RELATED TO NATIONAL SECURITY INFORMATION

All of the information discussed above relates, in one form or another, to national security. In light of the executive branch’s natural tendency toward secrecy in the national security context, and the unfettered discretion executive officials enjoy under the current regime, it is unlikely that the problems attendant to secrecy will improve absent congressional amendment of FOIA (directly or indirectly).\textsuperscript{113} There are many possible approaches, all of which would involve significant study.\textsuperscript{114} It is not the purpose of this Article to detail specific legislation. Rather, this section suggests three aspects of legislation necessary to ensure that FOIA’s purposes are served while still protecting national security.

First, Congress should establish a single, overarching, statutory framework governing classified, sensitive but classified, and critical infrastructure information.\textsuperscript{115} Such legislation can define terms, set standards for keeping information secret, determine the scope of the redefined FOIA exemption, and set forth terms of judicial review. Such an


\textsuperscript{113} See FOERSTEL, supra note 21, at 181 (“Only a fundamental change in the way information is classified can break the logjam [associated with secrecy], and the best possibility for reform rests with the [legislature].”). Such legislation may be direct in that all changes could be found in amendments to the language of exemption (b)(1). Or it may be indirect in that the (b)(1) exemption could reference a different statute that sets out most of the parameters discussed here.

\textsuperscript{114} Over the years, people have proposed a wide variety of legislation codifying guidelines to executive classification authority and withholding of information under FOIA. For a discussion of such proposals, see FOERSTEL, supra note 21, at 181-84 (describing Sen. Patrick Moynihan’s proposed “Government Secrecy Act of 1987”); Faust, supra note 65, at 641 (proposing an amendment to FOIA exemption 1); National Security and FOIA, supra note 19, at 421-22 (proposing that Congress legislate the substantive areas in which government information can be classified); Moorhead, supra note 17, at 108-11 (proposing creation of an independent “Classification Review Commission” with authority over the classification system); and Executive Privilege Hearings, supra note 45, at 293-98; id. at 312 (proposing “National Defense Data Classification Act of 1973”).

\textsuperscript{115} There are laws regarding FOIA exemptions of national security information beyond the three situations this Article discusses. For example, the Aviation and Transportation Security Act, 49 U.S.C. § 114 (Supp. I 2001), prohibits disclosure of sensitive transportation information and the CIA Information Act, 50 U.S.C. § 431 (2000) exempts CIA operational files from disclosure. This Article focuses on the three examples discussed herein because they withhold information based on general notions of national security. In contrast, the CIA and transportation security laws aim at specific contexts and agencies. That difference may or may not argue for separate treatment. One could quite possibly extend this Article’s framework to cover such situations. The point of this Article is to propose a framework that at a minimum brings together all general exemptions based on national security.
approach has significant advantages over the existing regime, which is currently a patchwork of definitions and standards from various (sometimes questionable) sources that lacks cohesiveness.\textsuperscript{116}

This framework would require Congress to review all national security information to determine (1) how current categorizations relate to one another, (2) whether secrecy with respect to each area is necessary, and (3) the relationship between judicial review and the executive claims of exemption. By reviewing and presenting the information as one body of work rather than in piecemeal fashion, Congress can better understand the body of knowledge currently being kept secret and act accordingly. In addition, codifying secrecy standards and FOIA exemptions together provides a continuity that is clearly missing from the current approach where changes in administration can effect drastic changes to information withholding.\textsuperscript{117} Such continuity provides greater clarity for bureaucrats making secrecy decisions and, ideally, will improve those decisions. Finally, an overarching statute will set a tone of openness that can permeate all withholding-related decisions, either through explicit statements or the general framework of standards prescribed.\textsuperscript{118} Currently, FOIA purports to set such a tone but all other official pronouncements regarding national security information emphasize the need for secrecy. By promoting openness in this framework statute, Congress could establish an important default setting against which executive officials work.\textsuperscript{119}

Second, the statute must, at a minimum, provide precise definitions and

\textsuperscript{116} Given the Supreme Court’s deference to executive decision-making in national security situations, see, United States v. Curtiss-Wright Export Corp., 299 U.S. 304 (1936) (explaining basis of federal power dealing with foreign affairs), some people will raise separation of powers arguments against the proposed statute. The Supreme Court has also indicated, however, that Congress can establish guidelines regarding the executive’s power to keep information secret. See EPA v. Mink, 410 U.S. 73, 83 (1973) (“Congress could certainly have provided that the Executive Branch adopt new procedures [regarding classification] or it could have established its own procedures—subject only to whatever limitations the Executive privilege may be held to impose upon such congressional ordering.”). While the separation of powers argument must be recognized during the crafting of legislation, it does not appear to prevent Congress from acting in this area.

\textsuperscript{117} See, e.g., Moorhead, supra note 17, at 102-05 (discussing criticism of Nixon order on classification); Note, Keeping Secrets: Congress, the Courts, and National Security Information, 103 HARV. L. REV. 906, 909-10 (1990) (discussing Reagan order).

\textsuperscript{118} President Carter’s executive order did this to some extent by requiring disclosure of even properly classified information unless that information could “reasonably be expected to cause identifiable harm to national security’ and ‘when the need to protect information outweigh[ed] the public interest in disclosure.’” See Exec. Order No. 12065, 3 C.F.R. 191 (1978). Congress could enact a similar provision. See Faust, supra note 65, at 641 (discussing proposed legislation with such a requirement).

\textsuperscript{119} Such changes promote the openness and accountability necessary to democracy. In this sense, the legislation operates as a “framework statute” as described by Bruce Ackerman. See Bruce Ackerman, The Emergency Constitution, 113 YALE L.J. 1029, 1077-78 (2004) (discussing APA as a framework statute that “sought to impose constitutional order on new and unruly realities” and which “imposed fundamental constraints on bureaucratic government in the name of democracy and the rule of law”).
standards for keeping information secret. With respect to definitions of information to be withheld, Congress should consider limiting secrecy to information related to "national defense" as opposed to the more amorphous notion of "national security." It is possible that the current entrenched notion of national security may render such a narrowing construction impossible (although the debate itself should prove worthwhile). In any case, Congress must establish precise definitions of the categories of information to be withheld. The Clinton and Bush orders provide reasonably good examples of such categorization. Even here, however, vague categories such as "scientific, technological, or economic matters related to" national security still exist and Congress should revisit them to determine if they can be narrowed. Precise definitions are especially important with respect to "sensitive but unclassified" information, which currently has no single definition and "critical infrastructure information" which is defined so broadly as to allow withholding of almost anything.

Congress should also precisely define classification standards. Current standards allow classification if information reasonably could be expected to cause "exceptionally grave damage," "serious damage," or "damage," to national security. Sensitive but unclassified information is usually kept confidential if it "adversely affects" certain national interests. Critical

---

120. See William G. Phillips, The Government's Classification System, in NONE OF YOUR BUSINESS: GOVERNMENT SECRECY IN AMERICA 61, 80-82 (Norman Dorsen & Stephen Gillers eds., 1974). Phillips suggests several other criteria that should be subject to legislation, such as the length of classification, declassification requirements, and mechanisms for internal review. Obviously, all such details are important. It is not clear, however, that they must be contained in legislation or whether Congress, after providing guidelines, could delegate specifics to an administrative entity such as an independent commission. See, e.g., President John F. Kennedy Assassination Records Collection Act of 1992, Pub. L. No. 102-526, 106 Stat. 3443 (1992) (establishing commission to oversee declassification of Kennedy assassination records). Definitions and standards regarding information to be withheld are too central to the abuse of secrecy for Congress to delegate.

121. See Executive Privilege Hearings, supra note 45, at 293-98 (citing proposal of William J. Florence).

122. Congress could limit classification to information necessary to protect specific foreign policy or national security objectives. National Security and FOIA, supra note 19, at 421-22. Such a limitation may curb the tendency to classify everything related to a category even when information does not pose a threat.


124. This assumes that Congress will use the "sensitive but unclassified" term in the disclosure context. One can make a strong argument that Congress should not use the term as it merely confuses issues regarding classification. If information poses a danger, it should be classified. If it does not, it should be subject to disclosure.

125. Senators Leahy, Levin, Jeffords, Lieberman, and Byrd proposed a bill limiting the critical infrastructure exemption to information regarding "the vulnerability of and threats to critical infrastructure (such as attacks, response and recovery efforts)," which provides a workable approach to narrowing the definition. See 149 CONG. REC. S3631-39 (daily ed. Mar. 12, 2003). The bill also remedies many of the defects in the current exemption discussed above. See supra notes 98-101 and accompanying text.
infrastructure information is exempt from disclosure because it has a “debilitating impact on security, national economic security, [or] national public health or safety.” All of these standards vary greatly. None of them provides much guidance. Congress should create a uniform standard(s) governing national security information. Such a standard might require, for example, that information can be classified when there are specific and articulable facts suggesting that disclosure of such information would cause identifiable harm to national security or critical infrastructure and that harm outweighs the public interest in disclosure. That standard provides coherence and guidance by requiring executive officials to focus on specific facts and weigh the harm against the need for public disclosure and may prevent overly broad classification of even non-threatening information simply because it is related to a category.126

Finally, Congress must encourage less deferential review regarding government claims of exemption under FOIA. It is not feasible for Congress to legislate stricter standards of review given that judges are supposed to review such claims de novo. Thus, Congress is left to change the accoutrements of de novo review. Most importantly, Congress should require in camera inspection of documents in national security cases rather than leaving it to judicial discretion, which many courts refuse to exercise. Such inspection would provide judges information that is often lacking in affidavits. As a result, judges might be more willing to question and overturn officials’ claims. Furthermore, the fact that Congress has firmly indicated its desire for more aggressive review of government claims may assuage judicial reticence in this area.127 Ultimately, the prospect of real scrutiny and the requirement of specific justifications as opposed to boilerplate recitations, may generally improve executive decisionmaking in this area.128

126. See Thomas Blanton, The World's Right to Know, FOREIGN POL’Y, Aug. 2002, at 50 (noting that nuclear weapons design and policies regarding nuclear weapons usage pose different threats to national security and that need for secrecy regarding the former might outweigh the public interest in disclosure while secrecy regarding the latter may not).
CONCLUSION

Excessive secrecy is and has been a genuine problem in the United States and is likely to worsen as threats of terrorism indefinitely continue. So strong is the pull of secrecy that one can plausibly argue the futility of statutory schemes and judicial review. After all, executive officials control this information in the first place and hold the upper hand in responding to requests. If they do not wish to disclose information, they can find ways to withhold it, regardless of whether it is properly classified. Excessive secrecy may thus be inevitable.

Surely, there is some truth to this argument. But declining to set legislative standards based upon it is a mistake. Legal mechanisms such as statutory requirements and judicial review are part of the overall backdrop against which officials make decisions to withhold information. Although such mechanisms provide no guarantee, without a strong presumption against secrecy, overzealous officials will inevitably withhold too much. Congressional standards thus send an important signal to resist the inevitable pull toward secrecy that threatens to engulf democratic notions of government premised upon openness and accountability. Such standards, even if “unlikely to be followed still may have some effect, in the long run, on what is or is not inevitable.”

129. See Stanley Futterman, What Is the Problem with Classification?, in None of Your Business, supra note 120, at 93, 95 (“An unclassified document can be hidden just as deeply in a file drawer . . . as a classified document can.”); see also Laura Gordon-Murnane, Access to Government Information in a Post 9/11 World, SEARCHER, June 2002, at 50 (recounting government official’s assessment that much withholding is driven by attitudes of officials rather than legal requirements).
130. SISSELLA BOK, SECRETS 181 (1982) (“[A] strong presumption against government control over secrecy” is necessary in order to escape “piecemeal dismantling” of FOIA).
** * * *