

Assessing the Health of FOIA After 2000 Through the Lens of the National Security Archive and Federal Government Audits*

Melissa Guy** and Melanie Oberlin***

Using audits by the National Security Archive and the General Accounting Office, the authors review the “state of health” of the Freedom of Information Act (FOIA) since 2000 in the context of increased national security concerns after the September 2001 attacks in the United States.

Introduction	331
Is 9/11 the Appropriate Benchmark?	333
Post-2000 Policy Instruments Concerning FOIA Administration	334
SBU Information and FOIA.	335
Auditing the FOIA Process.	338
The National Security Archive	338
National Security Archive Audit of FOIA	339
National Security Archive Audit of SBU	341
GAO Report: Agencies’ Views	342
Bush Administration Efforts to Improve the FOIA Process	344
Recent FOIA Legislation.	347
From SBU to CUI	348
The Obama Administration and FOIA.	350
Recommendations.	351
Considerations for Further Research	352
Appendix: Freedom of Information Act Exemptions	353

Introduction

¶1 The Freedom of Information Act (FOIA) has been a cornerstone policy instrument of open government in the United States for four decades. Since President Lyndon Johnson signed the FOIA in 1966, and the law came into effect on July 5, 1967, the act has guaranteed the right of access to records of federal executive agencies.¹ This right of access has always existed in tension with agencies’ need to withhold some government information in the interests of national secu-

* © Melissa Guy and Melanie Oberlin, 2009. The authors would like to thank Craig Blaha, Angela Crall, Philip Doty, Ed Sevcik, and Janet Sinder for helpful comments on earlier drafts.

** Social Sciences Liaison Librarian, Arizona State University, Tempe, Arizona.

*** Reference Librarian, Moritz Law Library, The Ohio State University, Columbus, Ohio.

1. Freedom of Information Act, Pub. L. No. 89-487, 80 Stat. 250 (1966) (codified as amended at 5 U.S.C. § 552 (2006)).

riety. While FOIA exemptions allow agencies to withhold information if its release is deemed to be a threat to national defense under criteria established by any relevant executive order,² the overall intent of the Act was to encourage broad disclosure.³

¶2 In the wake of the September 11, 2001, attacks in the United States, national security concerns have dominated politics, and have resulted in changes in the ways agencies control access to their records. In this article we evaluate recent changes in federal information policy concerning FOIA administration, with an emphasis on the policies of the George W. Bush administration in the wake of the attacks.

¶3 In considering the health of FOIA today, we relied heavily on the analyses and reports of the National Security Archive,⁴ a government watchdog organization and freedom of information advocate. Information on federal agencies' views of the FOIA process was taken from Government Accountability Office (GAO) and National Security Archive audits.⁵ In addition to examining the current FOIA process, we also look at alternative methods of restricting access to government information, such as the designation of "Sensitive but Unclassified (SBU) Information." SBU was described by the Information Security Oversight Office and Department of Justice (DOJ) Office of Information and Privacy as information related to U.S. homeland security that may not meet the standards of classifications set forth in Executive Order 12,958, issued by the Clinton administration on April 17, 1995.⁶ Our analysis found that the SBU designation is not clearly defined and erodes the intent and effectiveness of the Freedom of Information Act.

¶4 While a general commitment to FOIA among government agencies remains strong, administration guidelines, procedural challenges (e.g., backlogs), and the increased use of alternative designations (such as SBU) to restrict government information present a significant threat to the effectiveness of FOIA as a cornerstone policy instrument designed to reduce government secrecy and enable an informed citizenry.

2. Freedom of Information Act, 5 U.S.C. § 552(b)(1)(A) (2006).

3. *EPA v. Mink*, 410 U.S. 73, 80 (1973) (stating "[w]ithout question, the Act is broadly conceived" and citing legislative history materials to show that Congress intended full agency disclosure to the greatest extent possible).

4. See Nat'l Security Archive, <http://www.gwu.edu/~nsarchiv> (last visited Apr. 21, 2009). The Archive is discussed in more detail in ¶¶ 18–20 *infra*.

5. U.S. GEN. ACCOUNTING OFFICE, FREEDOM OF INFORMATION ACT: AGENCY VIEWS ON CHANGES RESULTING FROM NEW ADMINISTRATION POLICY (GAO-03-981 2003), available at <http://gao.gov/new.items/d03981.pdf>; NAT'L SECURITY ARCHIVE, THE ASHCROFT MEMO: "DRASTIC" CHANGE OR "MORE THUNDER THAN LIGHTNING"? (2003), available at <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB84/FOIA%20Audit%20Report.pdf> [hereinafter THE ASHCROFT MEMO]; NAT'L SECURITY ARCHIVE, PSEUDO-SECRETS: A FREEDOM OF INFORMATION AUDIT OF THE U.S. GOVERNMENT'S POLICIES ON SENSITIVE UNCLASSIFIED INFORMATION (2006), available at <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB183/SBU%20Report%20final.pdf> [hereinafter PSEUDO-SECRETS].

6. Memorandum from Laura L.S. Kimberly, Acting Director, Info. Security Oversight Office, Richard L. Huff & Daniel J. Metcalfe, Co-Directors, Office of Info. & Privacy, Dep't of Justice, to Departments and Agencies (Mar. 19, 2002), available at http://www.dod.mil/pubs/foi/dfoipo/docs/cbrn_wh_memo.pdf [hereinafter ISOO-DOJ Guidance Document]. The memo references Exec. Order No. 12,958, 3 C.F.R. 333 (1995) (Classified National Security Information). This memo was attached to a memorandum from Andrew H. Card, Jr., Ass't to the President and Chief of Staff, to the Heads of Executive Departments and Agencies (Mar. 19, 2002) [hereinafter Card Memo]. In 2008 the Bush administration attempted to replace SBU with the designation "Controlled Unclassified Information." See *infra* ¶¶ 41–44.

Is 9/11 the Appropriate Benchmark?

¶5 It is understandable that federal agencies would review their disclosure practices in the wake of an attack on U.S. soil; 9/11 is therefore an obvious place to begin an assessment of the health of FOIA. Yet evidence also suggests that a trend toward increased federal government secrecy began not on September 11, 2001, but with the inauguration of the Bush administration. According to Lotte Feinberg, “[c]oncerns about access to government records and secrecy under the George W. Bush Administration began almost immediately, and predated the September 11 attacks, although the attacks have been cited by the administration to justify much of this policy.”⁷ The National Security Archive reported: “Commentators ranging from senior Republican members of Congress to the Reporters Committee for Freedom of the Press have described a dramatic new trend towards increased government secrecy—predating the terrible events of September 11th, but escalating since then as the United States moved to a war footing.”⁸ The best place to begin assessing current changes in FOIA policy is the Justice Department FOIA policy memorandum issued by Attorney General Ashcroft on October 12, 2001.⁹ This memo, released less than one month after 9/11, combined with other policy instruments, such as Executive Order 13,233 of November 1, 2001,¹⁰ indicates that the trend toward secrecy began before 9/11.

¶6 One example of secrecy that clearly predates 9/11 is the disagreement that began in summer 2001 between Congress and the Cheney Energy Task Force over the task force’s refusal to release to GAO documents indicating when and with whom the task force met.¹¹ In general, though, pre-9/11 efforts to increase govern-

7. Lotte E. Feinberg, *FOIA, Federal Information Policy, and Information Availability in a Post-9/11 World*, 21 GOV’T INFO. Q. 439, 441 (2004).

8. THE ASHCROFT MEMO, *supra* note 5, at 3.

9. Memorandum from John Ashcroft, Attorney General, to Heads of All Federal Departments and Agencies (Oct. 12, 2001), available at <http://www.usdoj.gov/archive/oip/foiapost/2001foiapost19.htm> [hereinafter Ashcroft Memo].

10. Exec. Order No. 13,233, 3 C.F.R. 815 (2001). The order alters the procedure for release of Presidential Records pursuant to the Presidential Records Act of 1978 (Presidential Records Act of 1978, 44 U.S.C. §§ 2201-07 (2000)) and revokes a prior Executive Order implementing the Act (Exec. Order No. 12,667, 3 C.F.R. 208 (1989)). *Id.* at 819.

11. President George W. Bush created the National Energy Policy Development Group (NEPDG or “Cheney Energy Task Force”) in his second week of office and appointed Vice President Dick Cheney as the chairman. The purpose of the group was to develop an energy policy for the Bush Administration. T.J. Halstead, *The Law: Walker v. Cheney: Legal Insulation of the Vice President from GAO Investigations*, 33 PRESIDENTIAL STUD. Q. 635, 637 (2003). Critics of the Task Force’s reports raised concerns that representatives of the energy industry were given preferential access to the deliberations of the Task Force. Congressman Henry Waxman and John Dingell prompted the GAO to investigate the Task Force. *Id.* The administration refused to comply with GAO requests for documents that would have answered the questions about who was given access to the Task Force. Eventually, the GAO filed a lawsuit against the Task Force to obtain information, but this lawsuit was dismissed. *Walker v. Cheney*, 230 F. Supp. 2d 51 (D.D.C. 2002). Public interest groups trying to obtain the same information through FOIA requests then filed suit. The administration litigated the matter up to the United States Supreme Court rather than disclose with whom and when the Task Force met. *Cheney v. U.S. Dist. Court*, 542 U.S. 367 (2004). After remand from the Supreme Court, the case was dismissed. *In re Cheney*, 406 F.3d 723 (D.C. Cir. 2005). See generally Halstead, *supra*; Bruce P. Montgomery, *Congressional Oversight: Vice President Richard B. Cheney’s Executive Branch Triumph*, 120 POL. SCI. Q. 581 (2005–2006).

ment secrecy on the part of the executive branch are difficult to assess simply because the events of 9/11 were the basis of the administration's rhetoric that was subsequently used to explain nearly all governmental action in matters related to national security.

Post-2000 Policy Instruments Concerning FOIA Administration

¶7 Under FOIA, the U.S. DOJ is responsible for ensuring agencies' compliance with the Act.¹² At times, the attorney general issues policy memoranda regarding FOIA, especially at the beginning of a new presidential administration.¹³ Attorney General Ashcroft issued one such memorandum on October 12, 2001.¹⁴ This memorandum superseded the FOIA memorandum issued by Attorney General Janet Reno in 1993.¹⁵

¶8 The Ashcroft memo departed from the Reno memo in two significant ways. First, the Ashcroft memo stressed that when agencies make decisions about discretionary disclosure, agencies should carefully consider "protecting fundamental values that are held by our society," including "safeguarding national security, enhancing the effectiveness of law enforcement agencies," and "preserving personal privacy."¹⁶ It emphasized that disclosure of information protected under FOIA "should be made only after full and deliberate consideration of the institutional, commercial, and personal privacy interests that could be implicated by disclosure of the information."¹⁷ In effect, the memo advocated a presumption of non-disclosure. The Reno memorandum, on the other hand, established an overall "presumption of disclosure" and promoted discretionary disclosures to achieve "maximum responsible disclosure."¹⁸

¶9 The Ashcroft memorandum's second departure from the Reno memorandum concerned the DOJ's support of agencies' decisions to withhold information under the Act. Under the superseded Reno memorandum, DOJ had defended an agency's withholding information only "where the agency reasonably foresees that disclosure would be harmful to an interest protected by the exemption."¹⁹ The Reno standard is referred to as a "foreseeable harm" standard.²⁰ Following the Ashcroft memo, DOJ would defend an agency's withholding information under

12. 5 U.S.C. § 552(e)(5) (2006).

13. U.S. GEN. ACCOUNTING OFFICE, *supra* note 5, at 7. See also Susan Nevelow Mart, *Let the People Know the Facts: Can Government Information Removed from the Internet Be Reclaimed?*, 98 LAW LIBR. J. 7, 11, 2006 LAW LIBR. J. 1, ¶ 12 (citing Kristen Elizabeth Uhl, Comment, *The Freedom of Information Act Post-9/11: Balancing the Public's Right to Know, Critical Infrastructure Protection, and Homeland Security*, 53 AM. U. L. REV. 261, 269-70 (2003)).

14. Ashcroft Memo, *supra* note 9.

15. Memorandum from Janet Reno, Attorney General, to Heads of Departments and Agencies (Oct. 4, 1993), available at <http://www.gwu.edu/~nsarchiv/nsa/foia/reno93.pdf> [hereinafter Reno Memo].

16. Ashcroft Memo, *supra* note 9, at 1.

17. *Id.* at 1.

18. Reno Memo, *supra* note 15, at 1.

19. *Id.*

20. U.S. GEN. ACCOUNTING OFFICE, *supra* note 5, at 8.

any one of the nine exemptions to disclosure codified in FOIA if the agency had a “sound legal basis.”²¹

SBU Information and FOIA

¶10 In addition to a FOIA standard that now presumed against disclosure, the increased use of means other than the nine FOIA exemptions—such as protective marking for “sensitive” but unclassified information to restrict access to government information—has allowed for the circumvention of FOIA. One unprecedented source of executive branch guidance about sensitive information was Andrew Card, chief of staff for George W. Bush.²² On March 19, 2002, Card issued a memorandum to the heads of all executive departments and agencies headed “Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security.”²³ The Card memorandum called on departments and agencies to immediately reexamine measures for identifying and safeguarding records “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.”²⁴

¶11 As Card requested, the acting director of the Information Security Oversight Office (ISOO) and the co-directors of the DOJ’s Office of Information Policy provided guidance (“ISOO-DOJ Guidance”) that was attached to the Card memorandum giving more specific direction to the agencies. The ISOO-DOJ Guidance addressed information that was (1) classified, (2) previously unclassified or declassified, and (3) sensitive but unclassified (SBU). The ISOO-DOJ guidance describes SBU as, “sensitive information related to America’s homeland security that might not meet one or more of the standards for classification set forth in Part 1 of Executive Order 12,958.”²⁵ The ISOO-DOJ guidance document continues:

All departments and agencies should ensure that in taking necessary and appropriate actions to safeguard sensitive but unclassified information related to America’s homeland security, they process any Freedom of Information Act request for records containing such information in accordance with the Attorney General’s FOIA Memorandum of October 12, 2001, by giving full and careful consideration to all applicable FOIA exemptions.²⁶

¶12 The document explicitly links the SBU categorization to “applicable” FOIA exemptions, making a leap that does not have clear precedent in legal statute and is not implemented consistently among agencies. It appears that the Bush administration intended for SBU to constitute a de facto FOIA exemption with full backing from DOJ. The Card Memo states: “If they [agencies] need assistance in applying

21. Ashcroft Memo, *supra* note 9, at 1. See *infra* Appendix for the list of the nine exemptions to FOIA.

22. Feinberg, *supra* note 7, at 442 (“Perhaps the most unusual source of guidance came from Andrew Card, chief of staff for G.W. Bush—the only time any President’s chief of staff has ventured into this sensitive, substantive policy area.”).

23. Card Memo, *supra* note 6, at 1.

24. *Id.*

25. ISOO-DOJ Guidance Document, *supra* note 6, at 3.

26. *Id.*

exemptions of the Freedom of Information Act (FOIA) to sensitive but unclassified information, they should contact the Justice Department's Office of Information and Privacy (OIP)."²⁷ The memo's language suggests that agencies have broad discretion to employ SBU as a de facto exemption. If challenged, DOJ would defend the agency, finding a FOIA exemption to justify non-disclosure.

¶13 Congress has not defined "sensitive" unclassified information. The lack of definition has led to varying interpretations by different agencies.²⁸ In addition, for the class of material designated as SBU, there are no congressionally mandated procedures for appeal and review, or for reassessment of the designation.²⁹ In other words, individuals who are denied access to information deemed SBU have no explicit legal recourse to challenge a decision made by any number of employees at agency level, and it is unclear when, if ever, documents labeled SBU will be reassessed to determine the need for the label.

¶14 One of the sharpest contrasts between FOIA and the SBU regulations promulgated by various federal agencies is the use of the language governing the withholding of information. A Department of Homeland Security (DHS) Management Directive, issued May 11, 2004,³⁰ defines "For Official Use Only" (a category of SBU) information as that which "could" cause harm, instead of FOIA's standard of "reasonably expected" to cause harm.³¹ The DHS directive standard thus covers almost anything, including information that "could be sold for profit," "could result in physical risk," or "could constitute an indicator of U.S. government intentions, capabilities, operations, or activities or otherwise threaten operations security."³² While the DHS directive advises that the SBU designation does not automatically exempt the information from disclosure under FOIA, the entire document is couched in language restricting disclosure of SBU information other than on a "need to know" basis "in order to perform or assist in a lawful and authorized governmental function."³³ Agency guidance, such as the DHS directive, allows federal agencies to err on the side of extreme caution and consider virtually all information to be at risk of improper disclosure.

¶15 Whether the SBU designation is deemed equivalent to a FOIA exemption depends on its implementation. Apart from FOIA though, there is some evidence suggesting that the SBU categorization theoretically could *increase* access to gov-

27. Card Memo, *supra* note 6, at 2.

28. Feinberg, *supra* note 7, at 443 (citing GENEVIEVE J. KNEZO, "SENSITIVE BUT UNCLASSIFIED" AND OTHER FEDERAL SECURITY CONTROLS ON SCIENTIFIC AND TECHNICAL INFORMATION: HISTORY AND CURRENT CONTROVERSY (CRS Report No. RL31845, 2004), available at <http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-6031:1>).

29. *Id.* at 444.

30. DEP'T OF HOMELAND SECURITY, SAFEGUARDING SENSITIVE BUT UNCLASSIFIED (FOR OFFICIAL USE ONLY) INFORMATION (Management Directive System MD No. 11042, May 11, 2004), available at <http://www.fas.org/sgp/othergov/dhs-sbu.html> [hereinafter DIRECTIVE 11042]. This directive was superseded by DEP'T OF HOMELAND SECURITY, SAFEGUARDING SENSITIVE BUT UNCLASSIFIED (FOR OFFICIAL USE ONLY) INFORMATION, (Management Directive System MD No. 11042.1, Jan. 6, 2005), available at <http://www.fas.org/sgp/othergov/dhs-sbu-rev.pdf> [hereinafter DIRECTIVE 11042.1]. The language discussed was not changed in the newer version.

31. DIRECTIVE 11042, *supra* note 30, at 2; Feinberg, *supra* note 7, at 444-45.

32. Feinberg, *supra* note 7, at 445 (quoting DIRECTIVE 11042.1, *supra* note 30, at 4-5).

33. DIRECTIVE 11042.1, *supra* note 30, at 1-2.

ernment information by preventing the expansion of the use of classification. According to the State Department, SBU is and should be employed to “classified material to a minimum and to be able to pass-on relevant, but sensitive information to individuals . . . on a need to know bases (sic).”³⁴ In the process, federal agencies must have the authority to define SBU in ways that meet their institutions’ individual needs. The lack of a uniform definition of the concept safeguards freedom of information by *not* imposing blanket restrictions on access.³⁵ Yet no conclusive evidence exists to show that the use of SBU results in *fewer* classifications. SBU is often treated similarly to classified information, essentially creating a poorly defined fourth classification level.³⁶

¶16 Controlling access to agencies’ records through non-FOIA statutes, regulations, and guidance appears to be one way in which Congress and the Bush administration maneuvered after 2000. In the Homeland Security Act of 2002, Congress exempted Protected Critical Infrastructure Information from FOIA disclosure.³⁷ Congress also directed the President to “identify and safeguard homeland security information that is sensitive but unclassified.”³⁸

¶17 As part of the Intelligence Authorization Act for fiscal year 2003, Congress amended FOIA as it applies to records held by agencies in the intelligence community.³⁹ The changes prohibit agencies within the intelligence community and other agencies that have “elements” of intelligence from disclosing records requested directly or indirectly by non-U.S. government entities (foreign governments or international organizations). Fortunately, the changes are codified in FOIA,⁴⁰ but the new law deviates from the core FOIA concept of determining whether a record can be released, and focuses instead on trying to identify the requester and the intended use of the information.

34. KNEZO, *supra* note 28, at 17 (quoting Dep’t of State Telegram to All Diplomatic and Consular Posts, U.S. Office Pristina (Feb. 2, 2000), *available at* <http://www.fas.org/sgp/news/2000/02/sbu.html>).

35. *See id.* at 16.

36. *See id.* at 29–33. The U.S. Government has three classification levels: confidential, secret, and top secret. Exec. Order No. 12,958, 3 C.F.R. 333, 36 (1996), *amended by* Exec. Order No. 13,292, 3 C.F.R. 196, 196–97 (2004).

37. Homeland Security Act of 2002, Pub. L. No. 107-296, § 214(a)(1)(A), 116 Stat. 2135, 2135 (codified at 6 U.S.C. § 133(a)(1)(A) (2006)).

38. *Id.* § 892(a)(1)(B), 116 Stat. at 2153 (codified at 6 U.S.C. § 482(a)(1)(B) (2006)). “In 2003, President Bush delegated responsibility for protecting Sensitive Homeland Security Information (SHSI) to the Secretary of Homeland Security, but no regulations or other formalized SHSI protections have been implemented.” PSEUDO-SECRETS, *supra* note 5, at 2. In December 2005, President Bush issued a memorandum directing agencies to “develop standard procedures for handling . . . SBU information, including SHSI.” *Id.* As of 2006, no procedures had been disseminated. *Id.* A search by the authors for procedures developed after 2006 yielded no results.

39. Intelligence Authorization Act for Fiscal Year 2003, Pub. L. No. 107-306, § 312, 116 Stat. 2383, 2390 (2002).

40. 5 U.S.C. § 5(a)(3)(A), (E) (2006).

Auditing the FOIA Process

The National Security Archive

¶18 The National Security Archive is an independent non-profit research institute housed at George Washington University in Washington, D.C.⁴¹ As one of the primary advocates for open access to government records, the National Security Archive is a major stakeholder in changes in FOIA administration and related changes in restrictions to information, including SBU. Its staff regularly uses FOIA to request records from the U.S. government.⁴² As of 2002, National Security Archive staff sent out an average of five to seven FOIA requests per day, totaling more than 27,000 letters since 1985 and resulting in the acquisition of over five million pages of declassified documents available in the National Security Archive reading room. Many of the documents have also been published on microfiche, CD-ROM, the World Wide Web, and in book form.⁴³

¶19 According to the National Security Archive, the organization “systematically track[s] U.S. government agencies and federal records repositories for documents that either have never been released before, or that help to shed light on the decision-making process of the U.S. government and provide the historical context underlying those decisions.”⁴⁴ True to its name and its history, the National Security Archive devotes its resources to opening access to government records related to national security, especially information concerning U.S. foreign and intelligence policy.⁴⁵

¶20 The foundation for the National Security Archive was laid in the mid-1980s, with the formation of the Central American Project, created by journalist Raymond Bonner and Democratic Congressman Jim Moody from Wisconsin to gather information from FOIA requests about U.S. foreign policy. In 1985, *Washington Post* reporter Scott Armstrong sought to expand the project beyond Central America and obtained funding from several private foundations to start the National Security Archive.⁴⁶ The National Security Archive maintains an annual budget of approximately \$3.5 million,⁴⁷ generated primarily through publications and private grants; the Archive has a policy of not seeking U.S. government funding.⁴⁸ Examples of declassified documents obtained by the National Security Archive include records related to U.S. foreign policy in Afghanistan from

41. Nat'l Security Archive, *supra* note 4.

42. Nat'l Security Archive, About the National Security Archive, http://www.gwu.edu/~nsarchiv/nsa/the_archive.html (last visited Apr. 21, 2009).

43. Ron Chepesiuk, *National Security Archive Champions of Freedom of Information: FOIA Feeds a Vast Library of Declassified Documents*, AM. LIBR., Apr. 2002, at 80, 80.

44. Nat'l Security Archive, *supra* note 42.

45. The Archive does not confine its actions to foreign policy matters—as an advocate for open government in general, the organization was at the forefront of the legal effort to preserve e-mail records created during the Reagan, George H.W. Bush, and Clinton Administrations. *See id.*

46. Chepesiuk, *supra* note 43, at 82.

47. Nat'l Security Archive Fund, Inc., Financial Statements as of and for the Years then Ended December 31, 2007 and 2006 and Report Thereon 5 (2008), available at http://www.gwu.edu/~nsarchiv/nsa/audit_report_2007.pdf.

48. Nat'l Security Archive, *supra* note 42.

1973 to 1990, the Cuban Missile Crisis, the Iran-Contra affair, and apartheid in South Africa.⁴⁹

¶21 The implications of changes in FOIA policy for an organization such as the National Security Archive are difficult to measure. These difficulties are due, in part, to the fact that the Archive's public responses to changes in information policy tend to adopt a macroscopic approach that reflects the organization's overall commitment to open access to government records. That is to say, the National Security Archive does not always publish complaints regarding delays or other non-disclosure tactics related to specific requests. Nevertheless, the Archive's publications and other secondary sources related to FOIA policy changes can shed light on the possible implications of current policy trends for National Security Archive activity.

National Security Archive Audit of FOIA

¶22 In the wake of the Ashcroft memo of 2001, and to test the effect of the memo on the ability to access government records, the National Security Archive initiated a FOIA audit.⁵⁰ On September 3 and 4, 2002, the Archive filed FOIA requests with thirty-five federal agencies asking for information concerning the Ashcroft memo.⁵¹ In analyzing the agencies' responses, the National Security Archive studied: (1) the variety of correspondence generated from the request (letter, fax, e-mail, telephone); (2) documents received from the agency pursuant to the National Security Archive's FOIA request; (3) documents obtained from the agencies' FOIA web pages; and (4) notes from interviews of FOIA officials at selected agencies (officials all stated that the interviews were "not for attribution").⁵² In rating the impact of the Ashcroft memo on an agency, the National Security Archive considered the: "(1) scope of dissemination of [the] Ashcroft Memorandum; (2) change[s] in Agency regulations; (3) change[s] in Agency FOIA guidance; (4) change[s] in agency training materials; and (5) FOIA officials' descriptions of the impact [of the memo]."⁵³ Regarding implementation of the Ashcroft memo, the National Security Archive found:

- Five of thirty-three agencies (15%) "indicated significant changes in regulations, guidance, and training materials" and reported that the memo was widely disseminated.⁵⁴
- Eight agencies (24%) "indicated implementation activities" concerning the memo, including dissemination of the memo and incorporation into FOIA regulation and procedures.⁵⁵

49. See Chepesiuk, *supra* note 43, at 80.

50. See generally THE ASHCROFT MEMO, *supra* note 5.

51. The National Security Archive request to these thirty-five agencies sought: "All records, including but not limited to guidance or directives, memoranda, training materials, or legal analyses, concerning the [agency]'s implementation of U.S. Attorney General John Ashcroft's October 12, 2001, memorandum on the U.S. Freedom of Information Act." *Id.* at 5–6.

52. *Id.* at 6.

53. *Id.*

54. *Id.* at 11. These five agencies were: Department of the Air Force, Department of the Army, Department of the Navy, Department of the Interior, and Nuclear Regulatory Commission.

55. *Id.* at 14–15. These eight agencies were: Department of Commerce, Department of Defense,

- Seventeen agencies (52%) “indicated awareness and dissemination” of the memo, but “indicated little change in regulations, guidance, or training materials reflecting the new policy.”⁵⁶
- Three agencies (9%) “indicated no changes in regulations, guidance, or training materials, and little if no dissemination” of the memo.⁵⁷

¶23 The National Security Archive concluded that it had encountered stumbling blocks in the FOIA process that “make it extremely likely that the average member of the public will be frustrated, discouraged and ultimately unsuccessful in obtaining access to federal government records.”⁵⁸ The Archive also identified multiple problems with the FOIA process. Agency web sites, including DOJ’s “Principal FOIA Contacts at Federal Agencies,”⁵⁹ did not provide accurate or complete information for contacting the FOIA officer to make a request.⁶⁰ Agencies also failed to acknowledge requests within the twenty-business-day statutory time limit. The National Security Archive concluded that “most agencies are unable to substantively respond to a FOIA request” within that timeframe.⁶¹ Agencies lose FOIA requests. Three of thirty-five of the Archive’s requests were not in the agency’s FOIA processing systems when appeals were filed 99 to 100 days after the requests had been submitted.⁶²

¶24 FOIA backlogs are a serious problem. Responses to National Security Archive’s requests were not sent in many cases for well over 100 days or until after the National Security Archive filed an appeal after 100 days.⁶³ Delays are caused in part because many agencies have decentralized FOIA processing systems, thus hampering oversight, in addition to their inconsistent practices concerning administrative appeals.⁶⁴ Some agencies informed the National Security Archive that they did not accept administrative appeals for delayed responses, and that the Archive’s only remedy was to file a lawsuit. Agencies consistently instructed the National Security Archive that appeals filed due to a delayed response by the agency would only slow the processing of the request even further.⁶⁵ Finally, agencies did not cor-

Department of Justice, Department of State, Environmental Protection Agency, National Aeronautics and Space Administration, Office of Management and Budget, and Small Business Administration.

56. *Id.* at 18. These seventeen agencies were: Agency for International Development, Central Intelligence Agency, Drug Enforcement Administration, Defense Intelligence Agency, Department of Agriculture, Department of Education, Department of Energy, Department of Health and Human Services, Department of Housing and Urban Development, Department of Labor, Department of Transportation, Department of Treasury, Federal Bureau of Investigation, General Services Administration, National Archives and Records Administration, Office of Personnel Management, and Securities and Exchange Commission.

57. *Id.* at 20. These three agencies were: U.S. Central Command, Federal Emergency Management Agency, and National Science Foundation.

58. *Id.* at 29.

59. U.S. Dep’t of Justice, Principal FOIA Contacts at Federal Agencies, <http://www.usdoj.gov/oip/foiacontacts.htm> (last visited Apr. 27, 2009).

60. THE ASHCROFT MEMO, *supra* note 5, at 29.

61. *Id.* at 30.

62. *Id.* at 31.

63. *Id.* at 31–32.

64. *Id.* at 32–34.

65. *Id.* at 34.

rectly apply FOIA's fee categorization and fee waiver standards, which could prevent the public from obtaining government records or could increase the frequency of litigation if requesters have to sue in order for a court to review the agency's denial of a request for a fee waiver.⁶⁶

National Security Archive Audit of SBU

¶25 In 2006, the National Security Archive published the results of its audit of the federal government's policies on SBU.⁶⁷ The audit addressed two specific concerns: the impact of Andrew Card's memorandum and the ISOO-DOJ guidance document of March 19, 2002, and the breadth of the policies related to SBU information across the federal agencies. The National Security Archive used FOIA requests and research to determine the effects of the Card memo and discover the breadth of policies concerning SBU at thirty-seven agencies.⁶⁸ As can be seen in figure 1, the National Security Archive reported:

- Among all agencies, twenty-eight distinct policies existed for protection of unclassified information.⁶⁹
- Eight policies (29%), including that of the Department of Homeland Security, permit any employee in the agency to designate sensitive unclassified information; ten policies (35%) allow for senior or supervisory officials to designate; seven policies (25%) allow one named individual to oversee designation; and three policies (11%) do not clearly specify who may make designations.⁷⁰
- With regard to reversing the designation, twelve of the policies (43%) are unclear or do not specify how, and by whom, SBU markings can be removed.⁷¹
- Only seven policies (25%) include restrictions prohibiting use of the policy markings for improper purposes.⁷²

¶26 The National Security Archive audit calls attention to several important differences between FOIA and SBU information. First, allowing any employee to designate documents as SBU information allows for inconsistency in application. The Department of Homeland Security, for example, has 180,000 employees.⁷³ Second, the lack of clear specifications about when protective markings may be removed stands in marked contrast to the classification system, which provides for declassification after specified periods of time or the occurrence of specific events. Third, the lack of restrictions prohibiting use of SBU marking for improper purposes is different from the classification system, which explicitly prohibits classification for improper purposes. Finally, the National Security Archive found that there

66. *Id.* at 35. *See also* Freedom of Information Act, 5 U.S.C. § 552(a)(4)(A)(iii) (2006) (providing for waiver of fees for requests in the public interest); § 552(a)(4)(A)(vii) (providing for review by the court of an agency's denial of a request for waiver of fees).

67. NAT'L SECURITY ARCHIVE, PSEUDO SECRETS, *supra* note 5.

68. *Id.* at 1.

69. *Id.* at 12.

70. *Id.* at 15–16.

71. *See id.* at 17.

72. *Id.* at 20.

73. *See id.* at 18.

Authority to Designate Protected Information

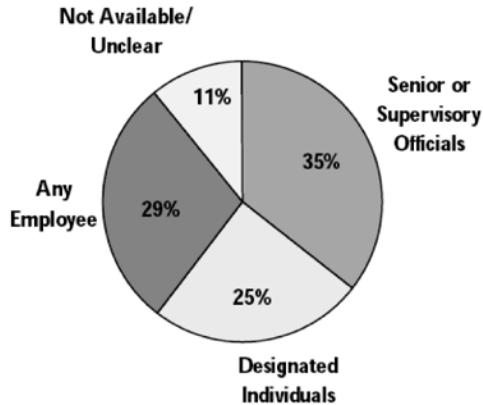


Figure 1. National Security Archive's SBU Audit Findings

Figure 1 reprinted with permission from NAT'L SECURITY ARCHIVE, *PSEUDO-SECRETS: A FREEDOM OF INFORMATION AUDIT OF THE U.S. GOVERNMENT'S POLICIES ON SENSITIVE UNCLASSIFIED INFORMATION* 14 (2003).

is no consistency among agencies about how they treat SBU information in the context of FOIA.⁷⁴ The overall conclusion of the National Security Archive audit was that procedures and regulations for safeguarding sensitive but unclassified information that were in use before September 11 "differed markedly from the post-September 11 regulations."⁷⁵

GAO Report: Agencies' Views

¶27 Beginning in 2002, the General Accounting Office (GAO) undertook a study to:

1. determine to what extent, if any, Justice guidance . . . on FOIA implementation has changed as a result of [the Ashcroft memo];
2. determine the views of FOIA officers at 25 agencies regarding the new policy and its effects, if any; and
3. determine the views of FOIA officers at 25 agencies regarding available FOIA guidance.⁷⁶

The GAO also obtained FOIA officers' views regarding the adequacy of guidance about sensitive information related to homeland security and critical infrastructure information.⁷⁷ The GAO reviewed DOJ guidance documents pertaining to FOIA and distributed a web-based and paper-based questionnaire between October 2002 and April 2003 to 205 FOIA officers at 25 agencies. The agencies chosen receive

74. *Id.* at ii.

75. *Id.*

76. U.S. GEN. ACCOUNTING OFFICE, *supra* note 5, at 9.

77. *Id.*

over 97% of FOIA requests. GAO had an 89% response rate (183 out of 205 FOIA officers), with at least one officer responding from 23 of 25 agencies.⁷⁸

¶28 GAO found that FOIA implementation documents promulgated by DOJ reflect the two points of difference between the Ashcroft and Reno memoranda.⁷⁹

Language referring specifically to the Reno memorandum was updated with references to the Ashcroft memorandum. For example, in the 2000 edition of the *FOIA Guide*, the following sentence appears:

- As a general rule, an agency's ability to make a discretionary disclosure of exempt information in accordance with Attorney General Reno's FOIA memorandum will vary according to the nature of the FOIA exemption and the underlying interests involved.

In the 2002 edition of the *FOIA Guide*, the sentence reads:

- As a general rule, an agency's ability to make a discretionary disclosure of exempt information as recognized in Attorney General Ashcroft's FOIA memorandum will vary according to the nature of the FOIA exemption and the underlying interests involved.⁸⁰

¶29 With regard to the use of discretionary disclosures, as is shown in figure 2, GAO found:

- Eighty-eight FOIA officers (48%) reported no change in their agencies' likelihood of making discretionary disclosures.
- Fifty-seven FOIA officers (48%) reported their agency was less likely to make discretionary disclosures; and of these officers, 75% "cited the new policy as a top factor influencing the change."
- Twelve FOIA officers (7%) reported their agency was more likely to make discretionary disclosures.
- Twenty-six FOIA officers (14%) reported they did not know or had no basis to judge, or they did not respond.⁸¹

78. *Id.* at 10–12.

79. *Id.* at 31.

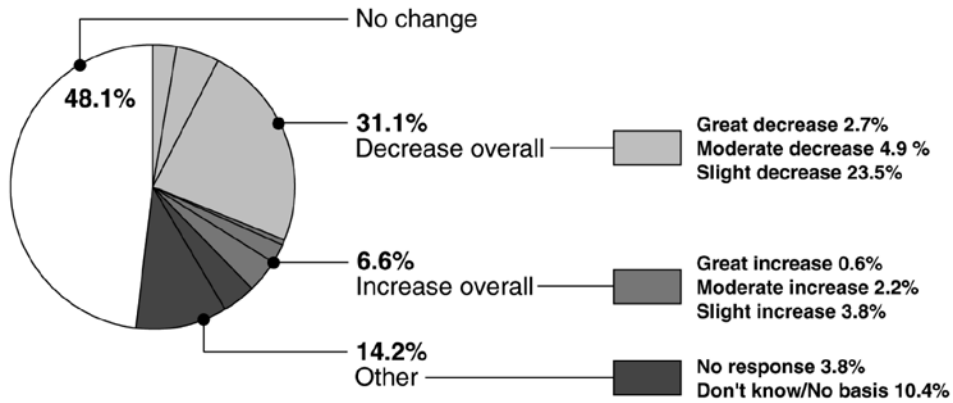
80. *Id.* at 19. The 2004 *FOIA Guide* maintains the 2002 changes and includes the following language:

The potential held by other FOIA exemptions for discretionary disclosure necessarily varies from exemption to exemption—but in all cases agencies should remember that any such action should be taken, as stated in Attorney General Ashcroft's FOIA Memorandum, "only after full and deliberate consideration of the institutional, commercial, and personal privacy interests that could be implicated by disclosure of the information."

For purposes of any discretionary disclosure that an agency considers, it also may be remembered that the FOIA requires agencies to focus on individual portions of records in connection with the applicability of all exemptions of the Act and to disclose all individual, "reasonably segregable" record portions that are not covered by an exemption.

Discretionary Disclosure and Waiver, in U.S. DEP'T OF JUSTICE, FREEDOM OF INFORMATION ACT GUIDE, MAY 2004 (2004), available at <http://www.usdoj.gov/oip/discretionary.htm>.

81. U.S. GEN. ACCOUNTING OFFICE, *supra* note 5, at 14.



Source: GAO.

Figure 2. Effect of Ashcroft Policy on Likelihood of Agencies' Making Discretionary Disclosures

Figure 2 courtesy of GAO. Excerpted from Gen. Accounting Office, Pub'n No. GAO-03-981, Freedom of Information Act: Agency Views on Changes Resulting From New Administration Policy (2003).

¶30 Regarding the use of specific FOIA exemptions, GAO found:

- One hundred and fourteen FOIA officers (62%) reported no change in the use of exemptions.
- Forty-five FOIA officers (25%) reported a change. "Most of these (28 of 45, or 62%) cited the new [DOJ] policy" as a main influence for change.⁸²

With regard to the adequacy of guidance documents, GAO found that fifty to seventy-five percent (depending on the particular type of guidance) of FOIA officers reported that guidance was adequate.⁸³

¶31 When asked to comment specifically on the adequacy of guidance related to sensitive homeland security information and critical infrastructure information, many (40–45%) FOIA officers "either did not respond . . . or reported that they had no basis to judge whether guidance and reference materials were adequate."⁸⁴

Bush Administration Efforts to Improve the FOIA Process

¶32 In Executive Order 13,392,⁸⁵ President Bush addressed the need to reduce FOIA request backlogs, improve customer service to FOIA requesters, and make

82. *Id.*

83. *Id.* at 15.

84. *Id.* at 37. The specific numbers of officers who had no response, didn't know or had no basis to judge the adequacy of guidance were: 42% on whether unclassified records contain sensitive information related to homeland security, 40% on whether to disclose sensitive information related to homeland security, 43% on judging whether materials is critical infrastructure information, 45% on judging whether to disclose critical infrastructure information.

85. Exec. Order No. 13,392, 3 C.F.R. 216 (2006).

other FOIA process improvements. The executive order sought to create a “citizen-centered” and “results-oriented” policy for improving the Act’s administration throughout the executive branch. It also required the attorney general to report to the President after review of individual agencies’ FOIA Improvement Plans mandated by the executive order.⁸⁶ In his initial report, Attorney General Alberto Gonzales stated that all agencies were following the executive order, which required a program review, an implementation plan, and the creation of reports under the direction of a Chief FOIA Officer.⁸⁷ Gonzalez also claimed that Executive Order 13,392 had an “immediate and widespread positive effect”⁸⁸ on the workings of agencies that administer FOIA. Gonzales especially praised the efforts of the Department of Defense for the “speed and quality of its early and sustained implementation efforts.”⁸⁹ Among the improvements “firmly embraced by the agencies” was the increased use of automation technology to confront backlogs.⁹⁰ Several agencies, including the Departments of Defense and Interior, sought to employ digital technologies to scan, redact, and process FOIA requests more quickly.

¶133 Despite the turn towards a presumption of nondisclosure as found in the Ashcroft and Card memos, the DOJ guidance for implementation of Executive Order 13,392 called for increased affirmative and proactive disclosures. Attorney General Gonzales lauded an increase in individual agencies’ FOIA web sites to improve efficiency and customer service. He also pointed to a greater emphasis on FOIA request status tracking through agencies’ new FOIA Requester Service Centers and FOIA Public Liaisons; the creation of customer service surveys and simplified “acknowledgment letters”; “in-house’ FOIA training”; and the elimination of backlogs through the “Ten Oldest FOIA Requests” initiative.⁹¹

¶134 Despite the fact that Executive Order 13,392 and Gonzales’s October 16, 2006, report attempted to address some of the concerns raised in the 2001 National Security Archive Audit, the National Security Archive released a statement on October 19, 2006, criticizing the administration’s approach to FOIA.⁹² In addition, the National Security Archive drafted formal letters to key members of the Senate Judiciary Committee and the House Government Reform Committee,⁹³ “calling for

86. *Id.* at 216, 219. FOIA Improvement Plans are the reports required by Section 3(b)(iv) of the Executive Order. Attorney General Alberto Gonzales coined the term in a report to the President. ATTORNEY GENERAL’S REPORT TO THE PRESIDENT PURSUANT TO EXECUTIVE ORDER 13,392, ENTITLED “IMPROVING AGENCY DISCLOSURE OF INFORMATION” 1 (Oct. 16, 2006), available at http://www.usdoj.gov/archive/oip/ag_report_to_president_13392.pdf [hereinafter ATTORNEY GENERAL’S REPORT].

87. Exec. Order No. 13,392, 3 C.F.R. at 218–19; ATTORNEY GENERAL’S REPORT, *supra* note 86, at 16.

88. ATTORNEY GENERAL’S REPORT, *supra* note 86, at 6.

89. *Id.* n.12.

90. *Id.* at 7.

91. *Id.* at 8–11.

92. Nat’l Security Archive, *Attorney General’s Report Ignores Serious Problems in Agency FOIA Programs: National Security Archive Calls for Congressional Oversight*, Oct. 19, 2006, <http://www.gwu.edu/~nsarchiv/news/20061019/index.htm>.

93. See, e.g., Letter from Meredith Fuchs, General Counsel, Nat’l Security Archive et al., to Sen. Arlen Specter, Sen. Patrick Leahy, and Sen. John Cornyn (Oct. 19, 2006), available at http://www.gwu.edu/~nsarchiv/news/20061019/Letter_to_Specter_Leahy_Cornyn.pdf [hereinafter Fuchs Letter].

congressional oversight hearings to make optimistic FOIA processing goals a reality.”⁹⁴

¶35 These letters called attention to “critical challenges facing the federal FOIA system” that the attorney general’s report ignored, including staffing, funding, and “cross-agency” leadership necessary for agencies to “bring their FOIA programs into compliance with the law.”⁹⁵ The Archive found that several agencies (e.g., Veterans Affairs) still had not updated their web sites to comply with the 1996 E-FOIA amendments, making it unlikely these same agencies would be able to address the requirements of Executive Order 13,322 in a manner consistent with the attorney general’s report. Moreover, efforts to reduce backlog must be based on a more accurate estimation of the problem. The National Security Archive did not believe that agencies were accurately reporting to Congress each year about their FOIA activities, and stressed that more personnel were necessary to address this problem. Finally, and most importantly for the health of FOIA, the National Security Archive warned against the perpetuation of a FOIA system that focuses primarily on “denying requests or finding reasons to reject requests.”⁹⁶ The letter argues: “A FOIA system that simply pushes papers and *does not release information of significance* costs money without providing the desired benefit of improved government accountability.”⁹⁷

¶36 In other words, an assessment of FOIA must consider the request process, but not at the expense of an honest consideration of *how* FOIA administration promotes access to government. The fact is that neither the executive order nor the attorney general’s report addressed matters beyond procedural concerns related to FOIA. Despite DOJ implementation guidelines that called for affirmative, proactive disclosure, Executive Order 13,392 did not supersede the Ashcroft and Card memos, which encouraged an increased use of FOIA exemptions, with the full weight of the DOJ supporting actions of nondisclosure.

¶37 On March 16, 2008, The National Security Archive released the results of a Knight Open Government Survey to determine how federal agencies had implemented Executive Order 13,392.⁹⁸ The survey found improvements had been made in overall customer service experiences during the request process: FOIA Service Centers, Public Liaisons, and Chief FOIA Officers at most agencies were responsive and helpful.⁹⁹ Still, the survey revealed that the executive order still lacked meaningful enforcement and resources, allowing agencies with already weak FOIA performance to continue their activities unchanged. Efforts at reducing backlogs produced mixed results. Of those agencies reporting backlogs at the time of the executive order, thirty percent of them reported an increase in the number of

94. Nat’l Security Archive, *supra* note 92.

95. Fuchs Letter, *supra* note 93, at 1.

96. *Id.* at 2.

97. *Id.* (emphasis added).

98. NAT’L SECURITY ARCHIVE, MIXED SIGNALS, MIXED RESULTS: HOW PRESIDENT BUSH’S EXECUTIVE ORDER ON FOIA FAILED TO DELIVER (2008), available at http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB246/eo_audit.pdf.

99. See *id.* at 4–5.

requests pending after 2006.¹⁰⁰ The number of pending requests across all agencies was only two percent lower at the end of 2007 than before the issuance of the executive order.¹⁰¹ Finally, Executive Order 13,392 has not improved agency web sites or compliance with E-FOIA.¹⁰²

Recent FOIA Legislation

¶138 Between 2000 and 2006, Congress was unable to pass legislation to strengthen FOIA. Proposals were made, but these could not move out of committee or secure enough votes for passage.¹⁰³ Fortunately, many of the provisions of these bills were reintroduced in a FOIA reform bill in the 110th Congress. The original bill took several forms, and ultimately passed as the Openness Promotes Effectiveness in our National (OPEN) Government Act of 2007.¹⁰⁴ The OPEN Government Act reiterates and emphasizes that disclosure is the dominant objective of FOIA and recognizes that Congress should regularly review FOIA to ensure that the government remains open and accessible to the American people under a “right to know” standard.¹⁰⁵ Among other things, the act also clarifies and strengthens the time limit for agencies to respond to requests, and establishes a tracking system for each request, which the public can use to monitor the status of outstanding requests.¹⁰⁶ The OPEN Government Act enhances the kind and amount of information that agencies must report annually to the attorney general concerning the agencies’ FOIA activities.¹⁰⁷ The Act creates an Office of Government Information Services within the National Archives and Records Administration.¹⁰⁸ This office is charged with reviewing agencies’ FOIA policies and procedures, auditing and reporting on agencies’ FOIA compliance, recommending FOIA policy to Congress and the President, and offering mediation services to requesters and agencies (an ombudsman function).¹⁰⁹

¶139 Unfortunately, a much needed provision was stripped out of the original bill (S. 849), and does not appear in the public law. That provision required any future statute (other than FOIA itself) that creates exemptions to disclosure under FOIA to specifically cite to the Freedom of Information Act.¹¹⁰ This provision

100. *See id.* at 6–7.

101. *Id.* at 11.

102. *Id.* at 16.

103. *See, e.g.*, Faster FOIA Act of 2005, S. 589, 109th Cong. (2005) (also introduced as H.R. 1620); OPEN Government Act of 2005, S. 394, 109th Cong. (2005) (also introduced as H.R. 867); S. 1181, 109th Cong. (2005); Restoration of the Freedom of Information Act, S. 609, 108th Cong. (2003).

104. OPEN Government Act of 2007, Pub. L. No. 110-175, 121 Stat. 2524 (amending 5 U.S.C. § 552 (2006)).

105. *Id.* § 2.

106. *Id.* §§ 6–7.

107. *Id.* § 8.

108. *Id.* § 10.

109. *Id.*

110. OPEN Government Act of 2007, S. 849, 110th Cong., § 8 (2007) (this bill was superseded by S. 2488, which became Pub. L. No. 110-175).

would prevent whittling away at FOIA, intentionally or unintentionally, by statutes that are difficult for FOIA proponents to track and monitor. Senators Leahy (D-VT) and Cornyn (R-TX) proposed new legislation in 2008¹¹¹ to address this needed legislative promise, but the bill died in committee. Fortunately, the two Senators have reintroduced the bill in the 111th Congress.¹¹²

¶40 Also, the Bush administration's proposed fiscal year 2009 budget attempted to move the functions of the new Office of Government Information Services, which includes the "FOIA Ombudsman," to the DOJ, away from the National Archives and Records Administration.¹¹³ This maneuver would have contravened the explicit text and the intent of the OPEN Government Act, which attempts to create an independent organ to mediate FOIA disputes between the public and the government. Fortunately, the 2009 budget passed without this Bush administration line item. The Office of Government Information Services remains part of the National Archives and Records Administration, as the Act intended, and has now been funded by the Obama administration budget.¹¹⁴

From SBU to CUI

¶41 On May 7, 2008, President Bush defined a new designation, "Controlled Unclassified Information (CUI)," to replace the SBU designation. The Bush administration defined CUI as:

unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.¹¹⁵

¶42 The CUI framework comprises three combinations of dissemination controls: (1) Controlled with Standard Dissemination; (2) Controlled with Specified Dissemination, and (3) Controlled Enhanced with Specified Dissemination.¹¹⁶ The National Archives and Records Administration (NARA) was charged with oversight and implementation of this new CUI framework and was given five years to implement it.¹¹⁷ To accomplish this task, NARA established the "Controlled

111. Open FOIA Act of 2008, S. 2746, 110th Cong. (2008).

112. Open FOIA Act of 2009, S. 612, 111th Cong. (2009).

113. See Patrick Leahy & John Cornyn, *Hopeful Signs for Your Right to Know*, ST. LOUIS POST-DISPATCH, Mar. 17, 2008, at B9.

114. See Omnibus Appropriations Act 2009, Pub. L. No. 111-5, 123 Stat. 523, 667; Nat'l Archives and Records Admin., President Approves \$459M Budget for National Archives, Mar. 7, 2009, <http://www.archives.gov/press/press-releases/2009/nr09-59.html>.

115. Memorandum on Designation and Sharing of Controlled Unclassified Information (CUI), 44 WEEKLY COMP. PRES. DOC. 673, 673-74 (May 7, 2008) [hereinafter CUI Memo].

116. *Id.* at 675.

117. *Id.* at 674, 675.

Unclassified Information Office.”¹¹⁸ No guidelines, policies, or procedures have yet to be established by the office.¹¹⁹

¶43 The CUI designation does nothing to alleviate the problems associated with SBU information. First, the memo allows each agency to establish policies for the designation,¹²⁰ continuing the inconsistent and confusing designations already present with SBU. Second, NARA is responsible for working with executive agencies to establish “penalties for improper handling of CUI,”¹²¹ but nothing in the memo indicates that there is a way to challenge those designations once they are made by executive agencies. Nor is there a de-designation procedure similar to declassification procedures for classified information, meaning that once information is designated CUI, it may remain so indefinitely, even when disclosure no longer poses any risks. Third, the scope of the applicability of CUI is not clear. It may replace all SBU designations, or it may replace SBU designation for only “terrorist information” as defined in the Intelligence Reform and Terrorism Prevention Act of 2004.¹²²

¶44 With respect to FOIA, the memo states that “CUI markings may inform but do not control the decision of whether to disclose or release the information to the public, such as in a response to a request made pursuant to the Freedom of Information Act”¹²³ As with SBU designations, open access advocates worry that CUI labels will become a *de facto* FOIA exemption.¹²⁴ Congressional committee investigation has found that a proliferation of pseudo-classification designations such as SBU or “for official use only” lack sufficient definition and control and can be used to prevent information sharing within the government and release of the information to the public.¹²⁵

118. Nat’l Archives and Records Admin., Archivist of the United States Establishes “Controlled Unclassified Information Office,” May 22, 2008, <http://www.archives.gov/press/press-releases/2008/nr08-107.html>.

119. See Nat’l Archives and Records Admin., Controlled Unclassified Information (CUI) Documents, <http://www.archives.gov/cui/documents> (last visited May 7, 2009).

120. CUI Memo, *supra* note 115, at 677.

121. *Id.* at 676.

122. According to the CUI Memo’s definition, CUI may apply to any unclassified information that is “pertinent to national interests of the United States or to the important interests of entities outside the Federal Government.” *Id.* at 674. However, other portions of the memo seem to limit the CUI classification to only that information previously labeled SBU that is part of the “Information Sharing Environment (ISE).” See, e.g., *id.* at 673. See also H.R. Rep. No. 110-810, at 2 (2008). ISE information is defined in the Intelligence Reform and Terrorism Prevention Act of 2004 as an approach to facilitate sharing of “terrorist information,” a term that is also defined by the Act. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1016(a)(2) (“Information Sharing Environment”), § 1016(a)(4) (“Terrorism Information”), 118 Stat. 3638, 3665.

123. CUI Memo, *supra* note 115, at 675.

124. See H.R. 6193, “The Improving Public Access to Documents Act of 2008”: Hearing Before the Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment of the H. Comm. on Homeland Security, 110th Cong. 14 (2008) (“any consideration of a CUI label in the FOIA process presents a true risk that the label may weight disclosure decisions against disclosure even when the FOIA exemptions would no longer apply”) (statement of Meredith Fuchs, General Counsel, Nat’l Security Archive).

125. See H.R. Rep. No. 110-779, at 7–8 (2008).

The Obama Administration and FOIA

¶145 While scholars may question whether FOIA should continue to be the cornerstone policy instrument for open government, at present it remains so. Just prior to submitting this article for publication, Barack Obama won the 2008 presidential election. President Obama declared FOIA “the most prominent expression of a profound national commitment to ensuring an open Government.”¹²⁶ The President immediately issued a memorandum reversing the position of the Bush administration on the issue of disclosure under FOIA, instructing the attorney general to issue new FOIA guidelines, and directing the director of the Office of Management and Budget to update guidance for agencies to increase and improve information dissemination to the public.¹²⁷

¶146 In response, Attorney General Eric Holder issued a Memorandum for Heads of Executive Departments and Agencies on March 19, 2009.¹²⁸ The Holder memo officially rescinded the Ashcroft memo of October 12, 2001, and described in clear language an expectation of a presumption of disclosure and proactive efforts to make government records available to the public. Contrary to DOJ practice under the Bush administration, the DOJ will now defend denial of FOIA requests under only two circumstances: (1) if the agency reasonably foresees that disclosure would harm an interest protected by one of the FOIA exemptions or (2) the disclosure is otherwise prohibited by law.¹²⁹ The Holder memo encourages agencies to respond to FOIA requests in a timely and efficient manner and to proactively disclose information online to reduce the need for members of the public to submit requests in order to obtain public information.¹³⁰

¶147 Open government advocates rightly celebrate the Obama administration’s early commitment to FOIA and open government. A return to a presumption of disclosure, which guided the FOIA policies of the Clinton administration, is a welcome change. Still, neither the Obama nor the Holder memos explicitly address alternative methods to restrict access to government information, namely, the categories of SBU and CUI. It also remains to be seen if the commitment to increasing efficiency, reducing backlogs, and encouraging proactive disclosure through the use of new technologies will be supported by necessary funding to carry out those tasks. Only in addressing SBU/CUI and other means of keeping government information secret, and by providing support for FOIA and other information dissemination methods, will the erosion of open government that began in 2000 be reversed. The challenge to the new administration, the remainder of the government, and the public to see that a new era of open government becomes a reality cannot be overstated.

126. Memorandum from Barack Obama, President, to Heads of Executive Departments and Agencies (Jan. 21, 2009), 74 Fed. Reg. 4683, 4683 (Jan. 26, 2009).

127. *Id.*

128. Memorandum from Eric Holder, Attorney General, to Heads of Executive Departments and Agencies (Mar. 19, 2009), available at <http://www.usdoj.gov/ag/foia-memo-march2009.pdf>.

129. *Id.* at 2.

130. *Id.* at 3.

Recommendations

¶148 Evidence from GAO and National Security Archive audits suggests that, while a general commitment to FOIA among government agencies remains strong, administration guidelines prior to 2009, procedural challenges (e.g., backlogs), and the increased use of alternative designations, such as SBU/CUI, to restrict government information present significant threats to the effectiveness of FOIA as an instrument designed to reduce government secrecy. The following recommendations are intended to address the current challenges faced by FOIA.

1. Congress should request that GAO update the 2003 GAO survey.¹³¹ An updated survey should consider the effects of DOJ guidance under the Bush and Obama administrations.
2. Legislation that amended FOIA without mentioning it or inserted amendments in the provisions of FOIA was a pernicious problem after 2000, because these amendments and the impact of the resulting legislation are difficult to monitor. The Open FOIA Act of 2009¹³² has been proposed to eliminate the possibility of amendments to FOIA that do not mention FOIA and are not codified in the provisions of FOIA. This bill should be supported by Congress, the public, and the President.
3. The government is required to attend to information policy in a time of rapidly changing technology, the increased availability of information, and security threats abroad and on U.S. soil. Much of Congress's time in recent years has been devoted to information policy, not to mention the time the executive branch agencies spend developing and implementing information policy. The OPEN Government Act of 2007 advances information policy by creating the Office of Government Information Services. This office must be adequately funded and staffed to support the development of modern information policy at Congress and in the agencies. A \$1 million allocation in the omnibus appropriations bill passed by Congress and signed by President Obama on March 11, 2009, is a good first step.
4. As requested by the National Security Archive, Congress should hold oversight hearings concerning FOIA based on reports completed pursuant to Executive Order 13,392 and the findings of the Knight Open Government Survey of March 2008. Special attention should be paid to those federal agencies with long histories of inadequate FOIA performance and those that are not compliant with E-FOIA.
5. Congress should conduct hearings on the increased use of alternative designations, such as SBU and CUI, that restrict access to government records. The goal of congressional oversight would be to eliminate those alternative designations, or at the very least, to ensure uniform SBU/CUI designation procedures, and development of an appeals process to challenge SBU/CUI designations. With a Congress controlled by the Democrats and the Obama administration's stated commitment to transparency and open government, the likelihood of hearings is increased.

131. U.S. GEN. ACCOUNTING OFFICE, *supra* note 5.

132. Open FOIA Act of 2009, *supra* note 112.

6. President Obama's and Attorney General Holder's calls for proactive disclosure to reduce backlogs and curb the need for FOIA requests must be supported by adequate funding and resources to facilitate making more records available to the public.

Considerations for Further Research

¶49 In addition to the recommendations outlined above, there are several other questions that call out for further inquiry. First, the October 2006 Attorney General Report noted more than a 35% increase in FOIA requests since Fiscal Year 2001.¹³³ Under these circumstances, we must consider whether the standard of non-disclosure as evidenced in the Ashcroft memo led to an increase in FOIA requests, thereby increasing the obvious problem of FOIA backlog. Second, audits of FOIA activity should go beyond procedural matters related to backlogs and notifications of requests. Specifically, it would be useful to determine if there is a pattern of new restrictions or significant changes in agencies handling FOIA requests from the National Security Archive about particular topics or foreign actors over others. Third, scholars should question whether FOIA is the right means to keep a public informed, considering that to request information, a member of the public must first know what kind of information is likely to exist and at what federal government entity. Instead, might a sophisticated, searchable, central clearinghouse of government information be more appropriate? Finally, more studies need to be done to reveal the circumstances under which particular FOIA exemptions are employed. As federal information policy scholars committed to FOIA's principles of open access to government records, we have a responsibility to monitor the health of legislation that remains the cornerstone of the public's "right to know."

133. ATTORNEY GENERAL'S REPORT, *supra* note 86, at 2.

Appendix

Freedom of Information Act Exemptions

Freedom of Information Act, 5 U.S.C.A. § 552(b) (West 2007 & Supp. 2008):

(b) This section does not apply to matters that are—

(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;

(2) related solely to the internal personnel rules and practices of an agency;

(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(5) inter-agency or intra-agency memorandums or letter which would not be available by law to a party other than an agency in litigation with the agency;

(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(9) geological and geophysical information and data, including maps, concerning wells.

Any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection. The amount of information deleted, and the exemption under which the deletion is made, shall be indicated on the released portion of the record, unless including that indication would harm an interest protected by the exemption in this subsection under which the deletion is made. If technically feasible, the amount of the information deleted, and the exemption under which the deletion is made, shall be indicated at the place in the record where such deletion is made.