

Testimony of John D. Podesta
President and CEO, Center for American Progress Action Fund
Before the Subcommittee on the Constitution
United States Senate
on
Secrecy and the Rule of Law
September 16, 2008

Executive summary

Most Americans appreciate the need to keep secret national security information whose disclosure would pose a genuine risk of harm. But as the 9/11 Commission concluded, too much secrecy can put our nation at greater risk, hindering oversight, accountability, and information sharing.

Excessive secrecy conceals our vulnerabilities until it is too late to correct them. It slows the development of the scientific and technical knowledge we need to understand threats to our security and respond to them effectively. It short-circuits public debate, eroding confidence in the actions of the government. It undermines the credibility of the information security system itself, encouraging leaks and causing people to second-guess legitimate restrictions.

The Commission on Protecting and Reducing Government Secrecy, chaired by Sen. Daniel Patrick Moynihan (D-NY), and on which I served, concluded that “The best way to ensure that secrecy is respected, and that the most important secrets *remain* secret, is for secrecy to be returned to its limited but necessary role. Secrets can be protected more effectively if secrecy is reduced overall.”

Government secrecy serves its proper and necessary function when it is reserved for situations in which there is an identifiable risk to national security. In other words, it should be used to keep secret only that which genuinely needs to be kept secret.

One of Sen. Moynihan’s key insights was that secrecy is really “a mode of regulation.” But it differs from more familiar forms of regulation in that “the citizen does not even know that he or she is being regulated. Normal regulation concerns how citizens must behave, and so regulations are widely promulgated. Secrecy, by contrast, concerns what citizens may know; and the citizen is not told what may not be known.”

The result, said Moynihan, is “a parallel regulatory regime with a far greater potential for damage if it malfunctions.”

Over the past seven years, the American people have come to understand what he meant. During this period, the Bush administration has increased secrecy and curtailed access to information through a variety of means, including by:

- Issuing an executive order that encouraged the overclassification of government information by shifting the presumption in favor of classification

- Slowing the pace of automatic and systematic declassification of government records, from a high-water mark of 204 million pages in 1997 during the Clinton administration to only 37 million in 2007
- Presiding over an explosion in the use of “controlled unclassified” markings, most of which have never been authorized by statute, to restrict access to unclassified information
- Withdrawing from public view thousands of pages of information that had previously been unclassified and available to the public through the Internet
- Interpreting the Freedom of Information Act in a manner that has undermined the presumption favoring disclosure
- Failing to preserve millions of White House communications as required by the Presidential Records Act and issuing an executive order that impedes the access of historians and the public to the records of past administrations
- Invoking executive privilege, the state secrets privilege, and other common law privileges, to cover up administration misdeeds and deny plaintiffs their day in court
- Threatening journalists, whistleblowers, and other private citizens with criminal prosecution for the possession or publication of national security information; and perhaps most egregious of all, the issuance of secret orders and legal opinions to shield illegal actions from public scrutiny

The obsessive secrecy of the Bush administration has damaged not only the security it was ostensibly meant to protect but also the rule of law that enables our society to maintain its internal stability and cohesion.

The rule of law can thrive only in an open society in which the laws are known and understood; government actions are taken, insofar as possible, in full view of the public and subject to scrutiny and debate; and government officials are held accountable for the arbitrary or unscrupulous exercise of power. The rule of law requires that Congress, the courts, the public, and the press have access to the information they need to serve as effective checks on the executive branch. Without such information, there can be no checks and balances. Unless the people know what their government is doing, there can be no rule of law.

My written testimony proposes a series of steps by which Congress and the next president can address each of these problems, and I welcome the opportunity to discuss them with you.

The key recommendations include the following:

- *Overclassification.* The next president should rewrite Executive Order 13292 to reinstate the provisions of Executive Order 12958 that establish a presumption against classification in cases of significant doubt, permit senior agency officials to exercise

- discretion to declassify information in exceptional cases where the need to protect the information is outweighed by the public interest in disclosure, and prohibit reclassification of material that had been declassified and released to the public under proper authority.
- *Controlled unclassified information.* At a minimum, the next president should issue a new memorandum that creates a presumption against the designation of controlled unclassified information, and Congress should enact legislation to reduce the use of unclassified information control markings and establish an orderly process that would discourage their misuse and maximize public access to unclassified information. Better still, Congress should give serious consideration to getting rid of these designations altogether.
 - *Freedom of Information Act.* The next president should direct the attorney general to revoke the Ashcroft memorandum and restore the presumption in favor of disclosure when there is no foreseeable harm to an interest protected by the exemption. If the president fails to take this step, Congress should amend FOIA to codify the presumption.
 - *Presidential records.* The next president should revoke Executive Order 13233, removing the ability of heirs and children of former presidents to block access to presidential records and eliminating the new vice presidential privilege. If the president does not act, Congress should amend the Presidential Records Act to codify this change. Congress also should enact legislation to tighten the standards and procedures for preservation of electronic records and to include enforcement measures for noncompliance.
 - *State Secrets Privilege.* Congress should consider statutory provisions to direct courts to weigh the costs and benefits of public disclosure in considering executive branch assertions of the State Secrets Privilege.
 - *Secret law.* The next president should direct the attorney general to issue a memorandum indicating that Office of Legal Counsel opinions will not be withheld from Congress under any theory of privilege, and that there will be a presumption of public disclosure unless disclosure would pose a genuine risk of harm to national security. Congress should enact S. 3405, the Executive Order Integrity Act, to make it unlawful for the president to secretly modify or revoke a published executive order.
 - *Whistleblower and press protections.* Congress should strengthen the Whistleblower Protection Act of 1989 to protect public employees from reprisal when they publicly disclose information regarding government wrongdoing or when they disclose classified information about government wrongdoing to members of Congress who are authorized to receive such information. Congress also should enact legislation to establish a qualified journalist-source privilege.

Taken together, these measures will help ensure that the government keeps secret only what needs to be secret. In so doing, they will enhance both openness and security while restoring respect for the rule of law. Thank you.

Secrecy and the rule of law

Thank you, Mr. Chairman, and members of the subcommittee. I am John Podesta, President and Chief Executive Officer of the Center for American Progress Action Fund. I am also a Visiting Professor of Law at the Georgetown University Law Center.

I served as Chief of Staff to President Bill Clinton from 1998 to 2001. I previously served in other roles in the White House, including Assistant to the President and Staff Secretary from 1993-1995, and Deputy Chief of Staff from 1997-1998.

I also have some experience in back of the dais, Mr. Chairman, having served as Counselor to former Senate Democratic Leader Tom Daschle, Chief Counsel for the Senate Agriculture Committee, and Chief Minority Counsel for the Senate Judiciary Subcommittees on Patents, Copyrights, and Trademarks; Security and Terrorism; and Regulatory Reform. It is an honor to be with you today.

* * *

Most Americans appreciate the need to keep secret national security information whose disclosure would pose a genuine risk of harm to our country and our people. This may include information on intelligence targets, sources and methods, military plans, troop movements and technology, and sensitive diplomatic negotiations.

But as the 9/11 Commission concluded, too much secrecy can put our nation at greater risk, hindering oversight, accountability, and information sharing.

Excessive secrecy conceals our vulnerabilities until it is too late to correct them. It slows the development of the scientific and technical knowledge we need to understand threats to our security and respond to them effectively. It short-circuits public debate, eroding confidence in the actions of the government. It undermines the credibility of the information security system itself, encouraging leaks and causing people to second guess legitimate restrictions. As Justice Stewart famously cautioned in the Pentagon Papers case:

I should suppose that moral, political, and practical considerations would dictate that a very first principle of that wisdom would be an insistence upon avoiding secrecy for its own sake. For when everything is classified, then nothing is classified, and the system becomes one to be disregarded by the cynical or the careless, and to be manipulated by those intent on self-protection or self-promotion. I should suppose, in short, that the hallmark of a truly effective internal security system would be the maximum possible disclosure, recognizing that secrecy can best be preserved only when credibility is truly maintained.¹

The Commission on Protecting and Reducing Government Secrecy, chaired by Sen. Daniel Patrick Moynihan, and on which I served, reached a similar conclusion in its 1997 report: “The

¹ N.Y. Times Co. v. U.S., 403 U.S. 713, 729 (1971) (Stewart, J., concurring).

best way to ensure that secrecy is respected, and that the most important secrets *remain* secret, is for secrecy to be returned to its limited but necessary role. Secrets can be protected more effectively if secrecy is reduced overall.”²

Government secrecy serves its proper and necessary function when it is reserved for situations in which there is an identifiable risk to national security.

One of Sen. Moynihan’s key insights was that secrecy is really “a mode of regulation.” But it differs from more familiar forms of regulation in that “the citizen does not even know that he or she is being regulated. Normal regulation concerns how citizens must behave, and so regulations are widely promulgated. Secrecy, by contrast, concerns what citizens may know; and the citizen is not told what may not be known.”

The result, said Moynihan, is “a parallel regulatory regime with a far greater potential for damage if it malfunctions.”

Over the past seven years, the American people have come to understand what he meant. During this period, the Bush administration has increased secrecy and curtailed access to information through a variety of means, including by:

- Issuing an executive order that encouraged the over-classification of government information by shifting the presumption in favor of classification;
- Slowing the pace of automatic and systematic declassification of government records, from a high-water mark of 204 million pages in 1997 during the Clinton administration to only 37 million in 2007;
- Presiding over an explosion in the use of “controlled unclassified” markings, most of which have never been authorized by statute, to restrict access to unclassified information;
- Withdrawing from public view thousands of pages of information that had previously been unclassified and available to the public through the Internet;
- Interpreting the Freedom of Information Act in a manner that has undermined the presumption favoring disclosure;
- Failing to preserve millions of White House communications as required by the Presidential Records Act and issuing an executive order that impedes the access of historians and the public to the records of past administrations;
- Invoking executive privilege, the state secrets privilege, and other common law privileges, to cover up administration misdeeds and deny plaintiffs their day in court;

² REPORT OF THE COMM’N ON PROTECTING & REDUCING GOV’T SECRECY (1997) at xxi.

- Threatening journalists, whistleblowers and other private citizens with criminal prosecution for the possession or publication of national security information; and perhaps most egregious of all, the issuance of secret orders and legal opinions to shield illegal actions from public scrutiny.

The obsessive secrecy of the Bush administration has damaged not only the security it was ostensibly meant to protect but also the rule of law that enables our society to maintain its internal stability and cohesion.

The rule of law can thrive only in an open society in which the laws are known and understood; government actions are taken, insofar as possible, in full view of the public and subject to scrutiny and debate; and government officials are held accountable for the arbitrary or unscrupulous exercise of power. The rule of law requires that Congress, the courts, the public and the press have access to the information they need to serve as effective checks on the executive branch. Without such information, there can be no checks and balances. Unless the people know what their government is doing, there can be no rule of law.

Overclassification, declassification, and reclassification

The Moynihan Commission recommended a series of statutory reforms to the classification system that were widely praised but never implemented. But the spirit of the Moynihan recommendations can certainly be discerned in the contemporaneous amendments to the classification system that were instituted by President Clinton under Exec. Order No. 12958.

The Clinton order established a presumption of access, directing that “If there is significant doubt about the need to classify information, it shall not be classified.” Similarly, the order provided that “If there is significant doubt about the appropriate level of classification, it shall be classified at the lower level.” The order also:

- Limited the duration of classification, providing that where the classifier cannot establish a specific point at which declassification should occur, the material will be declassified after 10 years unless the classification is extended for successive 10-year periods under prescribed procedures.
- Provided for automatic declassification of government records that are more than twenty five years old and have been determined by the Archivist of the United States to have permanent historical value, allowing for the continued classification of certain materials under specified procedures.
- Established a balancing test for declassification decisions in “exceptional cases,” permitting senior agency officials to exercise discretion to declassify information where “the need to protect such information may be outweighed by the public interest in disclosure of the information.”
- Prohibited reclassification of material that had been declassified and released to the public under proper authority.

- Authorized agency employees to bring challenges to the classification status of information they believe to be improperly classified.
- Created an Interagency Security Classification Appeals Panel (ISCAP) to adjudicate challenges to classification and requests for mandatory declassification, and to review decisions to exempt information from automatic declassification.

The changes instituted by President Clinton were largely erased by his successor, who issued a revised executive order in 2003. That order, Exec. Order No. 13292, eliminated the presumption of access, leaving officials free to classify information in cases of “significant doubt.” It also:

- Relaxed the limitations on the duration of classification, and made it easier for the period to be extended for unlimited periods.
- Postponed the automatic declassification of protected records 25 or more years old from April 2003 to December 2006, and permitted agencies to exempt certain categories of historical records from automatic declassification without a showing that the unauthorized disclosure would demonstrably damage the national security interests of the United States.
- Revived the ability of agency heads to reclassify previously declassified information if the information “may reasonably be recovered.”
- Allowed the Director of Central Intelligence to override decisions by ISCAP, subject only to presidential review.

The results of this shift in policy are reflected in the annual classification statistics published by the Information Security Oversight Office (ISOO) at the National Archives and Records Administration (NARA). According to ISOO’s 2007 report,³ executive branch agencies reported 23 million classification decisions in 2007, the overwhelming majority of which (22.8 million) were derivative classification decisions. This was nearly three times the number of classification actions (8.6 million) taken in 2001, the first year of the Bush administration, and four times the number (5.8 million) taken in 1996.

Estimates of the extent of over-classification vary, but the former director of ISOO, J. William Leonard, has cited an audit conducted by the Information Security Oversight Office which found that even trained classifiers, armed with the most up-to-date guidance, “got it clearly right only 64 percent of the time.”⁴

Unfortunately, we also know of instances in which over-classification is the result, not of honest error, but of a desire to conceal. The executive order governing classification prohibits the use of the classification system to “conceal violations of law, inefficiency, or administrative error” or

³ INFO. SEC. OVERSIGHT OFFICE, NAT’L ARCHIVES & RECORDS ADMIN., REPORT TO THE PRESIDENT 2007.

⁴ *Overclassification and Pseudo-classification: The Impact on Information Sharing: Hearing Before the Subcomm. on Intelligence, Information Sharing and Terrorism Risk Assessment of the House Comm. on Homeland Sec.*, 110th Cong. (2007) (statement of J. William Leonard).

“prevent embarrassment to a person, organization, or agency.” Yet at least some classification decisions by the Bush administration could have had little purpose other than to suppress information that might be embarrassing to the government.

A particularly egregious example is the infamous memo on interrogation of enemy combatants issued by the Office of Legal Counsel in 2003 and only declassified on March 31, 2008. According to Mr. Leonard, the memorandum should never have been classified in the first place: “The document in question is purely a legal analysis,” and contains “nothing which would justify classification.”⁵

Another notorious example is the decision by the Department of Defense to classify in its entirety the March 2004 report of the investigation by Maj. Gen. Antonio M. Taguba of alleged abuse of prisoners by members of the 800th Military Police Brigade at Baghdad’s Abu Ghraib Prison. According to an investigation by the Minority Staff of the House Committee on Government Reform:

One reporter who had reviewed a widely disseminated copy of the report raised the issue in a Defense Department briefing with General Peter Pace, the Vice Chairman of the Joint Chiefs of Staff, and Secretary Rumsfeld. The reporter noted that ‘there’s clearly nothing in there that’s inherently secret, such as intelligence sources and methods or troop movements’ and asked: ‘Was this kept secret because it would be embarrassing to the world, particularly the Arab world?’ General Pace responded that he did not know why the document was marked secret. When asked whether he could say why the report was classified, Secretary Rumsfeld answered: ‘No, you’d have to ask the classifier.’⁶

The desire to prevent embarrassment seems also to have played a role in the Bush administration’s aggressive reclassification campaign. According to a February 2006 report by the National Security Archive, the administration had reclassified and withdrawn from public access as of that date 9,500 documents totaling 55,500 pages, including some that are over 50 years old. For example:

- A complaint from the Director of Central Intelligence to the State Department about the bad publicity the CIA was receiving after its failure to predict anti-American riots in Colombia in 1948.
- A document regarding an unsanctioned CIA psychological warfare program to drop propaganda leaflets into Eastern Europe by hot air balloon that was canceled after the State Department objected to the program.
- A document from spring 1949, revealing that the U.S. intelligence community's knowledge of Soviet nuclear weapons research and development activities was so poor

⁵ Federation of American Scientists, Secrecy News, Apr. 3, 2008.

⁶ MINORITY STAFF OF HOUSE COMM. ON THE JUDICIARY, 10TH CONG., REPORT ON SECRECY IN THE BUSH ADMINISTRATION (2004) at 50.

that America and Britain were completely surprised when the Russians exploded their first atomic bomb six months later.

- A 1950 intelligence estimate, written only 12 days before Chinese forces entered Korea, predicting that Chinese intervention in the conflict was “not probable.”⁷

These reclassification actions call to mind the observations of the late Erwin N. Griswold, former Solicitor General of the United States and Dean of Harvard Law School, who argued the Pentagon Papers case before the Supreme Court in 1971. Presenting the case for the government, he had argued that the release of the Pentagon Papers would gravely damage the national security. Nearly two decades later, Griswold reflected on the lessons of that case:

It quickly becomes apparent to any person who has considerable experience with classified material that there is massive overclassification and that the principal concern of the classifiers is not with national security, but rather with governmental embarrassment of one sort or another. There may be some basis for short-term classification while plans are being made, or negotiations are going on, but apart from details of weapons systems, there is very rarely any real risk to current national security from the publication of facts relating to transactions in the past, even the fairly recent past. This is the lesson of the Pentagon Papers experience, and it may be relevant now.⁸

Some of the unclassified material removed from government web sites after 9/11 was at least more plausibly related to contemporary security concerns. But agencies have failed to provide a convincing rationale for how the withholding of these records serves the public interest.

Consider, for example, the Risk Management Plans (RMPs) which are reported by chemical companies to the Environmental Protection Agency. These plans contain accident histories, measures adopted to prevent chemical releases, disaster plans, and worst-case scenario data, including the number of people in surrounding areas at risk of being killed or injured in the event of a catastrophic release.

More than two years *before* 9/11, the FBI was asked by the chemical industry to determine whether the disclosure of this information would increase our vulnerability to terrorism. At the Bureau’s advice, Congress blocked EPA from disseminating the worst-case scenario assessments through the Internet (although these remain available at 50 reading rooms around the country). However, the FBI determined that the remaining information presented no increased risk and could remain on EPA’s web site.

⁷ MATTHEW M. AID, NAT’L SEC. ARCHIVE, DECLASSIFICATION IN REVERSE: THE U.S. INTELLIGENCE CMTY’S SECRET HISTORICAL DOCUMENT RECLASSIFICATION PROGRAM (2006).

⁸ Erwin N. Griswold, *Secrets Not Worth Keeping: The Courts and Classified Information*, WASH. POST, Feb. 15, 1989, at A25.

Ultimately, the FBI's determination mattered little. All RMP information came down in EPA's post-9/11 sweep, and it has yet to be restored. The public has been given no real explanation as to why.

In taking such actions, the administration has considered only the risks of public disclosure, not the benefits. Removing information does not remove risk, and may even increase it, lulling the public into a false sense of security and preventing citizens from bringing pressure to bear on officials responsible for chemical security.

The Bush administration has failed to act aggressively to address the problem.⁹ Secrecy is a poor substitute for policies that would make us more secure.

Recommendations regarding overclassification

It is, of course, too late to prevent the Bush administration from making classification decisions in violation of its own executive order. But the next president can swiftly rewrite the executive order to reinstate the provisions of Exec. Order No. 12958, specifically:

1. Establish a presumption against classification in cases of significant doubt;
2. Permit senior agency officials to exercise discretion to declassify information in exceptional cases where the need to protect the information is outweighed by the public interest in disclosure; and
3. Prohibit reclassification of material that had been declassified and released to the public under proper authority.

In addition, the new order should require agencies to (a) consider the harm to the public interest (and to national security) of classifying information, (b) require that information be classified at the lowest level and the shortest duration appropriate, (c) confine classification to those portions of the document that are properly classified, and (d) establish systems for oversight, training and auditing of classification decisions, and remedies for improper classification decisions.

Controlled unclassified information (pseudo-classification)

For all its faults, the classification system has many virtues as well. Classification actions are subject to uniform legal standards pursuant to executive order. These actions can be taken by a limited number of officials who receive training in the standards to be applied; they are of

⁹ See, e.g., Paul Orum, *Toxic Trains and the Terrorist Threat*, Center for American Progress, Apr. 2, 2007, available at http://www.americanprogress.org/issues/2007/04/chemical_security_report.html; Preventing Toxic Terrorism, Center for American Progress, available at http://www.americanprogress.org/issues/2006/04/b681085_ct2556757.html; Linda Greer, *New Strategies to Protect America: Securing our Nation's Chemical Facilities*, Center for American Progress, available at <http://www.americanprogress.org/kf/chemplantsecurity.pdf>.

limited duration and extent; they are monitored by a federal oversight office; they can be challenged; and they can be appealed.

The same cannot be said for the potpourri of unclassified control markings used by federal agencies to manage access to sensitive government information, most of which are defined by neither statute nor executive order, and which collectively have come to be known pejoratively as the “pseudo-classification” system.

Among the better known are Sensitive But Unclassified (SBU), Sensitive Security Information (SSI), Sensitive Homeland Security Information (SHSI), Critical Infrastructure Information (CII), Law Enforcement Sensitive (LES), and For Official Use Only (FOUO). While some of these control markings are authorized by statute,¹⁰ others have been conjured out of thin air. Some of these pseudo-classification regimes allow virtually any agency employee (and often private contractors) to withhold information without justification or review, without any time limit, and with few, if any, internal controls to ensure that the markings are not misapplied.

A March 2006 report by the Government Accountability Office (GAO) found that the 26 federal agencies surveyed use 56 different information control markings (16 of which belong to one agency) to protect sensitive unclassified national security information. The GAO also found that the agencies use widely divergent definitions of the same controls.¹¹

As in the case of classification and reclassification actions, these designations have at times been used not to protect legitimate national security secrets, but to spare the government from embarrassment. In a March 2005 letter to Rep. Christopher Shays, then the Chairman of the House Committee on Government Reform, Rep. Henry Waxman cited examples in which:

- The State Department withheld unclassified conclusions by the agency’s Inspector General that the CIA was involved in preparing a grossly inaccurate global terrorism report.
- The State Department concealed unclassified information about the role of John Bolton, Under Secretary of State for Arms Control, in the creation of a fact sheet that falsely claimed that Iraq sought uranium from Niger.
- The Department of Homeland Security concealed the unclassified identity and contact information of a newly appointed TSA ombudsman whose responsibility it was to interact daily with members of the public regarding airport security measures.
- The CIA intervened to block the chief U.S. weapons inspector Charles A. Duelfer, from revealing the unclassified identities of U.S. companies that conducted business with Saddam Hussein under the Oil for Food program.

¹⁰ See, e.g., Aviation and Transp. Sec. Act, Pub. L. No. 107-71; Fed. Info. Sec. Act, Pub. L. No. 107-347; Homeland Sec. Act, Pub. L. No. 107-296; Critical Infrastructure Info. Act, Pub. L. No. 107-296.

¹¹ U.S. GOV’T ACCOUNTABILITY OFFICE, REP. NO. GAO-06-385, INFORMATION SHARING: THE FEDERAL GOVERNMENT NEEDS TO ESTABLISH POLICIES AND PROCESSES FOR SHARING TERRORISM-RELATED AND SENSITIVE BUT UNCLASSIFIED INFORMATION (2006).

- The Nuclear Regulatory Commission sought to prevent a nongovernmental watchdog group from making public criticisms of its nuclear power plant security efforts based on unclassified sources.¹²

In May 2008, President Bush issued an executive memorandum¹³ establishing a framework for the sharing of controlled unclassified information, which purported to standardize practices and thereby improve the sharing of information but in fact does nothing to limit the use (and misuse) of what are now collectively referred to as “controlled unclassified information” (CUI).

Recommendations regarding controlled unclassified information

At a minimum, the next president should issue a new memorandum that creates a presumption against the designation of controlled unclassified information. But Congress can and should go further. The House has passed two bills, H.R. 6193, introduced by Rep. Jane Harman (D-CA), and H.R. 6576, introduced by Rep. Henry Waxman (D-CA), which seek to reduce the use of unclassified information control markings and establish an orderly process that would discourage their misuse and maximize public access to unclassified information.

Enactment of this or similar legislation would be a positive step. Congress also might usefully resurrect the limitations on unclassified controls contained in H.R. 5112, the Executive Branch Reform Act, which was reported by the House Government Reform Committee during the 109th Congress. Those provisions would have prohibited agencies from adopting unclassified controls that are not expressly authorized by statute or executive order, except where the Archivist determines that there is a need for some agencies to use such designations “to safeguard information prior to review for disclosure.”

Legislation to eliminate non-statutory CUI markings would begin to ameliorate some of the worst features of what is today an unregulated wilderness of inconsistent standards and insufficient checks. But such proposals beg the question of whether Congress should be conferring such power on agency officials in the first place. Such measures are all too easy to enact, and once they are in place, it is virtually impossible to get rid of them.

I would therefore urge Congress to give serious consideration to getting rid of these designations altogether. If the information is sensitive enough to meet the test for classification, it should be classified. If it cannot meet that test and does not fall within a specific FOIA exemption, then it should be available to the public.

The Freedom of Information Act

¹² H.R. Rep. No. 109-18, at 16 (2005) (letter from Rep. Henry Waxman to Rep. Christopher Shays).

¹³ *Memorandum for the Heads of Executive Departments and Agencies re: Designation and Sharing of Controlled Unclassified Information (CUI)* (May 9, 2008), available at <http://www.whitehouse.gov/news/releases/2008/05/20080509-6.html>.

In the decades since its enactment in 1966, the Freedom of Information Act (FOIA) has been one of the principal means by which the citizens of the United States can obtain access to unpublished government information. Under the statute, agencies are permitted to withhold information only if it is covered by one of the nine categories that are exempt from disclosure.

In 1993, Attorney General Janet Reno issued a memorandum which announced that in determining whether or not to defend a nondisclosure decision under FOIA, the Department of Justice would apply a “presumption of disclosure,” and would defend the assertion of an exemption “only in those cases where the agency reasonably foresees that disclosure would be harmful to an interest protected by that exemption.”¹⁴

In 2001, Attorney General Ashcroft issued a new memorandum, superseding the Reno memorandum and replacing the “foreseeable harm” standard with a much less stringent standard requiring only a “sound legal basis” for the assertion of a FOIA exemption.¹⁵ Not surprisingly, agencies have responded to the Ashcroft memo by making aggressive use of the exemptions to deny requests.

Equally troubling are the enormous backlogs in the handling of FOIA requests. While FOIA requires agencies to provide an initial response to a request within 20 days and to provide the documents in a timely manner, agencies often take months or years to respond. A 2007 survey of 87 agencies by the National Security Archive found that one requester has been awaiting a response for 20 years, and 16 have been waiting more than 15 years.¹⁶

In December 2007, President Bush signed the OPEN Government Act, Public Law No: 110-175, which codified long-sought reforms to create incentives to improve agency response times and limit redactions, expand the definition of “news media” who are exempt from search fees, and require government contractors who maintain information “that would be an agency record” to respond to FOIA requests, and improve agency reporting requirements.

Recommendations on FOIA

One key provision of the OPEN Government Act that was dropped in the course of negotiations would have reversed the Ashcroft memo. The next president should direct the attorney general to issue a memorandum revoking the Ashcroft memorandum and restoring the presumption in favor

¹⁴ *Memorandum for Heads of Departments and Agencies re: The Freedom of Information Act* (Oct. 4, 1993), available at <http://www.fas.org/sgp/clinton/reno.html>.

¹⁵ *Memorandum for Heads of All Departments and Agencies re: The Freedom of Information Act* (Oct. 12, 2001), available at <http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm>.

¹⁶ NATIONAL SECURITY ARCHIVE, *20 YEARS OF FOIA, 20 YEARS OF DELAY: OLDEST PENDING FOIA REQUESTS DATE BACK TO THE 1980S*, July 2, 2007, available at <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB224/index.htm>.

of disclosure when there is no foreseeable harm to an interest protected by the exemption. If the president fails to take this step, Congress should amend FOIA to codify the presumption.

Presidential records

After resigning the presidency, Richard Nixon sought to retain personal control over his presidential records and to shield them from public view. Congress responded by enacting the Presidential Records Act of 1978 (PRA), which provides that presidential records are the property of the United States, and requires the president to “take all such steps as may be necessary to assure that the activities, deliberations, decisions, and policies that reflect the performance of his constitutional, statutory, or other official or ceremonial duties are adequately documented and that such records are maintained as Presidential records.”

In 2001, President Bush issued E.O. 13233, which seriously undermined the intent of the PRA by granting the heirs and children of former presidents the right to block release of presidential records. It also created a new vice presidential privilege.

The Bush administration has also failed in its statutory duty to preserve many of the records of its own tenure. After the Clinton White House struggled to recover more than a million electronic files that had not been properly archived by its automated records management system, it left office with an effective electronic records management system in place. The new administration proceeded to replace that system with one that was both less reliable and less secure. The new system led to the loss of millions of emails over an 18-month period from January 2003 to July 2005. An internal analysis by the White House found approximately 700 days on which one or more components of the EOP reported an unusually low number of emails. For 473 of those days, one or more components reported no emails at all. There were 12 days for which no emails generated by the president’s immediate office could be found, and 16 days without any emails generated by the office of the vice president.

In addition, it was learned that over 80 senior White House officials, including senior adviser Karl Rove, had routinely circumvented the archiving system altogether by conducting official business through their Republican National Committee email accounts. Most of these emails were not preserved, and congressional investigators found that little or no effort had been made to recover them.

The “loss” of millions of email messages leaves a major gap in the historical record, compromising the ability of historians to understand how and why crucial decisions were made. It presents a serious obstacle to historians and ordinary citizens seeking to understand the course of events and the actions and motivations of those who participated in them.

For this reason, the Center for American Progress asked 30 of the nation's most eminent historians to join us in urging Congress to enact legislation to strengthen the Presidential Records

Act.¹⁷ In a letter to [House](#)¹⁸ and [Senate](#)¹⁹ leaders (attached), they argue that such reforms are essential to ensure that presidential records are preserved for posterity. Their call for reform has been endorsed by the three leading associations of U.S. historians: the American Historical Association, the Organization of American Historians, and the National Coalition for History.

Recommendations on Presidential Records

The next president should revoke Exec. Order. 13233, removing the ability of heirs and children of former presidents to block access to presidential records and eliminating the new vice presidential privilege. Without the executive order, management and release of presidential records would once more be governed by existing NARA regulations (36 C.F.R. 1270). The regulations provide procedures for the incumbent president to dispose of records after obtaining the views of the Archivist. They offer an outgoing president the opportunity to restrict certain types of records from disclosure for 12 years, and provide former presidents with notice and an opportunity to assert claims that the records are privileged and should not be disclosed.

If the president fails to act to revoke E.O. 13233, Congress should act by approving legislation along the lines of S. 886/H.R. 1255, the Presidential Records Act Amendments of 2007, bipartisan legislation introduced by Sen. Jeff Bingaman (D-NM) and Rep. Henry Waxman (D-CA).

The House of Representatives has already passed one measure that would begin to address the problem of preservation of electronic records, although its prospects in the Senate are uncertain. H.R. 5811, The Electronic Communications Preservation Act, introduced by Rep. Henry Waxman (D-CA), would require the archivist to issue standards for preservation of electronic records and to report to Congress on whether agencies are complying with them. The bill also would require the archivist to establish electronic records management standards for presidential records, and to certify annually whether the controls established by the president meet the requirements.

H.R. 5811's congressionally mandated standards and reporting requirements would be a step in the right direction. But I would urge Congress to go further. The bill includes no real enforcement measures, and affords no remedy if the president fails to comply. At a minimum, Congress should provide a statutory role for the Archivist of the United States in ensuring White House compliance. Congress also should consider provisions which would empower the

¹⁷ Mark D. Agrast, *Congress Must Act to Preserve Presidential Records for Future Generations*, Center for American Progress, Sept. 8, 2008, available at

http://www.americanprogressaction.org/issues/2008/presidential_records_act.html.

¹⁸ *Letter from U.S. Historians to House leaders* (Sept. 5, 2008), available at http://www.americanprogressaction.org/issues/2008/pdf/presidential_records_act1.pdf.

¹⁹ *Letter from U.S. Historians to Senate leaders* (Sept. 5, 2008), available at http://www.americanprogressaction.org/issues/2008/pdf/presidential_records_act2.pdf.

archivist and the public to challenge future presidents or vice presidents who fail to honor their obligation to preserve the nation's history for future generations.

More immediately, before the current administration leaves office, Congress should seek an acknowledgment from the vice president that, notwithstanding his prior assertions that he is not a member of the executive branch, he is bound by the record retention requirements of the Presidential Records Act, which require that vice presidential records be treated “in the same manner as Presidential records.”²⁰

Executive branch privileges

The Bush administration has made aggressive use of executive privilege claims to withhold information from Congress and the courts. In addition, it has repeatedly asserted the common law state secrets privilege to curtail judicial review of government actions.

Executive privilege

The text of the Constitution says nothing about the right of Congress to demand information from the executive branch—or the right of the executive to withhold it. Yet the Supreme Court has long recognized that the power to investigate and the attendant use of compulsory process are inherent in the legislative function vested in the Congress by Article I of the Constitution.²¹

Our system of checks and balances requires that Congress have the ability to obtain the information it needs to make the laws and to oversee and investigate the activities of the executive branch. And it also requires that the president have the ability to resist demands for disclosures of information that could threaten important national interests, particularly disclosures that would harm the national security or foreign relations of the United States, and including those that would jeopardize ongoing criminal investigations or interfere with his ability to obtain frank and candid advice.

President Clinton from time to time invoked the privilege when he felt it was necessary to protect presidential communications and deliberations from overly broad and intrusive requests for information. But he also understood that the privilege is not unqualified: the public interests protected by the claim of privilege must be weighed against those that would be served by the disclosure. He appreciated that even where the privilege applies, it is not absolute. It can be overcome by a strong showing that the information request is focused, that Congress does not have other practical means of obtaining the information, and that the information is genuinely

²⁰ 44 U.S.C. § 2207.

²¹ e.g. *McGrain v. Daugherty* 273 US 135 (1927); *Sinclair v. United States* 279 U.S. 263 (1929); *Watkins v. United States* 354 U.S. 178 (1957)

needed by the Committee and is “demonstrably critical to the responsible fulfillment of the Committee’s functions.”²²

Some in the present administration appear to believe that presidential advisers are immune from giving testimony on the theory that Congress does not have jurisdiction to oversee the Office of the President. No president in our country’s history has attempted to make such an extraordinary claim and no precedent provides a legal justification to support that assertion.

That is what Judge Bates has thus far concluded in regard to the current controversy over the refusal of former White House Counsel Harriett Miers to testify before the House Judiciary Committee. And it is what I would expect the courts to continue to say, at least to the extent that the two branches are unable to resolve these matters for themselves through the normal process of accommodation.

State secrets privilege

The state secrets privilege was recognized by the Supreme Court in *Reynolds v. U.S.*, 345 U.S. 1 (1953), in which the executive branch sought dismissal of a suit brought under the Federal Tort Claims Act by the families of civilians killed in the crash of an B-29 Air Force plane. The families sought to gain access to the accident reports, but the government asserted in court that the national security would be harmed if the case were allowed to proceed. The Court accepted the government’s claims but failed to inquire sufficiently to determine whether the claims were legitimate.

Decades later, when the documents were declassified, it was revealed that the plane had a history of mechanical failures and accidents, and the Air Force had failed to carry out preventive maintenance that might have prevented the disaster. The Court had been deceived: the government had asserted the state secrets privilege not to protect national security but to prevent its negligence from coming to light.

From the *Reynolds* case to the present day, the state secrets privilege has been repeatedly employed, not to protect genuine state secrets, but to shield the government from political and legal accountability for its misdeeds. Yet with few exceptions, the courts have continued to accord extraordinary deference to the mere assertion of the privilege, abandoning their proper role in reviewing the government’s claims.

The nine presidents who served from 1953 to 2001 claimed the state secrets privilege just 55 times. Since 9/11, the Bush administration has invoked the privilege more than 20 times. These instances included:

²¹ See *Senate Select Committee on Presidential Campaign Activities v. Nixon*, 498 F.2d 725 (D.C.Cir. 1974).

- Challenges to the president's warrantless surveillance program brought by the American Civil Liberties Union, the Electronic Frontier Foundation, and the Center for Constitutional Rights.
- Lawsuits brought by Khaled El-Masri, a German citizen abducted by the CIA in Macedonia and rendered to Afghanistan, where he was tortured; and Maher Arar, a Canadian seized in a U.S. airport and rendered to Syria, where he too was subjected to torture.
- A whistleblower suit brought by Sibel Edmonds, a former Turkish translator for the FBI, who was dismissed after attempting to alert her supervisors to problems in the division.

Recommendations on privilege claims

The next president and the next Congress undoubtedly will experience conflicts regarding requests for information. There will be times when each branch is compelled to assert its prerogatives. But the potential for such collisions can be considerably reduced, and those that occur can be more speedily resolved, if both branches avoid drawing lines in the sand. The next president would be wise to reject the radical doctrinal absolutism advanced by the outgoing administration, and both branches would do well to seek a resolution of these conflicts through the usual process of accommodation.

Given the tendency of many courts to defer to state secrets claims without examining them, it is important for Congress to adopt legislation to provide real judicial review. Congress should consider statutory provisions, such as those contained in S. 2533, the State Secrets Protection Act, reported by the Senate Judiciary Committee in August 2008, to provide real judicial review of the government's assertion of the State Secrets Privilege by directing the courts to weigh the costs and benefits of public disclosure.

Secret law

There is surely nothing more repugnant to the rule of law in a democracy than the secret enactment or revocation of the laws themselves. If the laws are not knowable, then there is no way for the people to follow them, or to know whether their government is following them.

Executive orders

The leading case we know about was the president's secret order authorizing the National Security Agency to intercept the international electronic communications of American citizens without a court order. This action was a violation of the Foreign Intelligence Surveillance Act, and as an executive order cannot override a statute, was plainly illegal. But it also was inconsistent with Exec. Order 12333, first issued by President Reagan in 1981, and amended by later presidents, including President Bush, which establishes the framework of rules and institutional structures that govern the U.S. intelligence community.

The Office of Legal Counsel has taken the position—secretly, of course—that since the president may revoke or modify an executive order at any time, he may do so simply by departing from it, rather than by expressly waiving or revoking it. This at last puts into effect the famous remark of President Nixon—“If the President does it, that means that it is not illegal.”

Thus, while President Bush has formally amended E.O. 12333 on three occasions, under the theory of his administration, he also has amended it tacitly on at least one occasion we know about, and perhaps many others that have yet to come to light. This means that Exec. Order 12333 is not, in fact, a statement of current law at all.

It is one thing to say that the president may amend his own orders—a proposition on which there is no disagreement. It is another thing to say that he and his administration are not bound by those orders, and may simply suspend their operation for one day only while leaving them officially on the books. It is particularly revealing of this administration’s overweening conception of executive power and its contempt for the rule of law that it sees nothing wrong with this.

As a practical matter, this practice makes oversight impossible and greatly complicates the task of legislating. How can Congress oversee the executive branch if it does not even know what orders and legal rulings are in effect? How can Congress enact new laws if it does not know how the existing laws are being interpreted and applied?

It is fundamentally inconsistent with the rule of law for the government, like any other business, to maintaining two sets of books, one public, the other for its eyes only. Nothing is more corrosive of public confidence in the rule of law.

OLC memoranda

The same must be said of opinions issued by the Office of Legal Counsel—authoritative interpretations of the Constitution and the laws on which the executive branch relies in making policy decisions. The president has fought to keep numerous OLC opinions secret under various theories of executive privilege. These include opinions long sought by this committee regarding the legality of the president’s warrantless surveillance program, the interrogation of persons declared enemy combatants and many other matters.

It is one thing for the president to seek to maintain the confidentiality of documents that track the deliberations of his close advisers. It is another thing for him to withhold from congressional overseers the definitive legal interpretations which form the basis for the actions of the administration.

Recommendations on secret law

The next president should direct the attorney general to issue a memorandum indicating that OLC opinions, as binding authority on the executive branch, will not be withheld from Congress under any theory of executive privilege, deliberative process privilege or attorney-client privilege, and that there will be a presumption of public disclosure of such opinions unless their disclosure would pose a genuine risk of harm to national security.

Congress should enact S. 3405, the Executive Order Integrity Act, which was introduced by you, Mr. Chairman, and Senator Whitehouse, to make it unlawful for the president to secretly modify or revoke a published executive order. Under your legislation, the bill would require the president to provide notice in the Federal Register within 30 days after he “revokes, modifies, waives, or suspends a published Executive Order or similar directive.” Such a notice would be required to specify the order affected by the president’s action and the nature of the change, so that there would be no ambiguity about what precise provisions are in effect. The bill would not compel publication of any information that is classified, but would require that such information be provided to Congress.

I hope that Congress approves this important yet modest proposal, and that the next president signs it. I also hope the next president and his Justice Department will repudiate the obnoxious view that the president may modify a published executive order simply by acting inconsistently with it, rather than by formally revoking, amending or waiving it. The president must be bound by the law or it is not the law.

Protections for whistleblowers and the press

The rule of law requires that government be accountable to the people. And this in turn depends in large part on the vigor, courage and diligence of the media and private citizens, including nongovernmental watchdog organizations and conscientious actors within the government itself. While unauthorized disclosures can be exceedingly harmful to our national security, these are best handled through clear standards and administrative enforcement, not through threats and reprisals against the press or other nongovernmental actors.

Protections for whistleblowers

By revealing information about illegal activities by government officials and contractors, whistleblowers serve as an important check against official wrongdoing. It is in the public interest to ensure that they come forward, and that they do not face retaliation when they do so.

Protections for journalists

The U.S. does not have an Official Secrets Act. In 2001, President Clinton vetoed the 2001 Intelligence Authorization bill because it contained an official secrets provision that would have made any “unauthorized” disclosure of classified information a felony. Prior to 9-11, the Bush Administration took a public position consistent with the views expressed by President Clinton.

But subsequently, the Bush administration has not been deterred. It has aggressively sought to transform the 1917 Espionage Act into the next best thing.

The Espionage Act prohibits the unauthorized disclosure of classified defense information to enemy powers with the intent to harm the United States. It does not apply to publication of classified information by the media. Yet Attorney General Alberto Gonzales darkly hinted that journalists who publish such information could be prosecuted under the Act. The Bush administration also attempted to use the Act to force the American Civil Liberties Union to turn over a leaked three-and-a-half-page document that apparently contained no classified information but may have been embarrassing to the government. Had this effort succeeded, it would have marked the first time in history that a criminal grand jury subpoena was used to force a private recipient of leaked material to turn it over to the government.

The Justice Department also has sought to bring pressure on journalists who refuse to disclose their confidential sources. It has had reporters jailed for refusing to cooperate with leak inquiries. Congress has under consideration legislation which would recognize a qualified journalist-source privilege that seeks to weigh the interest of the public, on one hand, in discouraging leaks that harm the national security, and on the other hand, in encouraging the media to tell the public things which the government may not wish them to know.

Recommendations on protections for whistleblowers and the press

Congress should enact S. 274, the Federal Employee Protection Act, which was introduced by Senator Daniel Akaka (D-HI) and passed by the Senate in December 2007. The bill would strengthen the Whistleblower Protection Act of 1989 to protect public employees from reprisal when they publicly disclose information regarding government wrongdoing. It also would protect employees who disclose classified information about government wrongdoing to members of Congress who are authorized to receive such information.

Congress also should enact S. 2035, the Free Flow of Information Act, introduced by Sens. Specter and Leahy and reported by the Senate Judiciary Committee on October 22, 2007. The bill would recognize a qualified journalist-source privilege, prohibiting compelled testimony by journalists unless the court determines that the testimony is essential to a criminal investigation or prosecution and cannot be obtained in any other way, that the matter concerns an unauthorized disclosure of properly classified information which will cause significant, clear and articulable harm to the national security, and that nondisclosure of the information would be contrary to the public interest.

Secrecy and e-government

Given the many threats and challenges we face as a nation, it is imperative that we enlist the full potential of new technologies to alert the public and enlist its cooperation and support in

reducing risk and improving our quality of life. The culture of secrecy embraced by this administration is antithetical to that effort, and ultimately self-defeating.

New information technologies make it possible to gather, analyze, and disseminate large volumes of data. Sensor and satellite technology provide the ability to collect data remotely—in real-time, with no paper reporting necessary—on almost anything in the physical environment. Electronic reporting systems allow data to be delivered and aggregated instantaneously. Data-mining programs apply automated algorithms to extract patterns and correlations that might take years to uncover manually. And all of this information can be shared through the Internet in accessible, searchable formats that allow journalists, academics, nongovernmental organizations and concerned citizens to perform their own independent analyses.

The Center for American Progress has put forward recommendations to harness these technologies to build an open and accountable data-driven government.²³ The Bush administration, unfortunately, has been headed in the opposite direction.

EPA's Toxics Release Inventory, a publicly searchable Internet database, demonstrates the power of information to promote health and safety improvements. Since its launch 20 years ago, industrial releases of the original 299 toxic chemicals tracked by TRI have declined nearly 60 percent, due in large measure to public pressure and heightened awareness within government and industry itself.

Unfortunately, instead of building on this success, the administration has revoked disclosure requirements at the urging of industry lobbyists. In December 2006, EPA finalized a rule that exempts thousands of facilities from fully accounting for their toxic releases.²⁴ Specifically, facilities are now permitted to use the program's less informative "short form" for small quantities of persistent bioaccumulative toxins (PBTs)—which includes lead, mercury, and dioxin—as well as releases of other TRI chemicals up to 2,000 pounds (the previous threshold was 500 pounds).²⁵

Similarly, the National Highway Traffic Safety Administration (NHTSA) answered the wishes of the auto industry when it decided, in 2003, to withhold "early warning" data about automobile safety defects, which Congress required to be reported after the widespread failure of Firestone tires in 2000. NHTSA made the dubious claim that disclosure of this information—including warranty claim information, auto dealer reports, consumer complaints, and data on child restraint systems and tires—could result in "substantial competitive harm" to the auto industry.²⁶ On Sept.

²³ Daniel C. Esty and Reece Rushing, *Governing by the Numbers*, Center for American Progress, April 23, 2007, available at http://www.americanprogress.org/issues/2007/04/data_driven_policy.html.

²⁴ 71 Fed. Reg. 76932 (Dec. 22, 2006)

²⁵ EPA went even further in its original proposal. In particular, the agency proposed to scrap annual reporting entirely in favor of biennial reporting, but backed off in the face of strong opposition from Sen. Lautenberg and others.

²⁶ 68 Fed. Reg. 44209 (July 28, 2003)

10, NHTSA finally made some of this information available through SaferCar.gov following successful lawsuits by Public Citizen.²⁷

Such disclosure advances the rule of law by allowing the public to verify compliance and observe whether government and private-sector actors are serving the common good. With advances in information technologies, we now have the tools to greatly expand disclosure and accountability. It is to be hoped that the next administration, unlike the current one, views this as an opportunity rather than a threat.

Conclusion

Thank you again for convening this hearing and inviting me to participate in it. I hope that Congress and the next president will act to ensure that the government keeps secret only the information that needs to be secret. In so doing, they will enhance both openness and security while restoring respect for the rule of law. Thank you.

²⁷ NHTSA is still withholding the number of consumer complaints to the manufacturer, field reports taken, and claims involving death and injury.