



# governmentattic.org

*"Rummaging in the government's attic"*

Description of document: Copies of certain Department of Justice (DOJ) views letters from the 101st through the 109th Congresses, 1996-2005

Requested date: 14-February-2011

Released date: 08-May-2013

Posted date: 01-February-2016

Source of document: FOIA Request  
Chief, Initial Request Staff  
Office of Information Policy  
Department of Justice  
Suite 11050  
1425 New York Avenue, NW  
Washington, DC 20530-0001  
Fax: (202) 514-1009  
[Online FOIA Request Form](#)

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



**U.S. Department of Justice**  
Office of Information Policy  
*Suite 11050*  
*1425 New York Avenue, NW*  
*Washington, DC 20530-0001*

---

*Telephone: (202) 514-3642*

May 8, 2013

Re: OLA/11-00427 (F)  
VRB:DRH:ND

This responds to your Freedom of Information Act (FOIA) request dated and received in this Office on February 14, 2011, in which you requested copies of certain views letters from the 101<sup>st</sup> through the 109<sup>th</sup> Congresses. This response is made on behalf of the Office of Legislative Affairs.

Please be advised that a search has been conducted in the Office of Legislative Affairs and 152 pages of material were located that are responsive to your request. I have determined this material, which provides the Department's views on the Terrorism Bill of 1996, the Electronic Freedom of Information Improvement Act of 1996, the Government Secrecy Act of 1997, the Counterintelligence Reform Act of 2000, National Security Intelligence Improvement Act of 2004, Homeland Security Federal Workforce Act of 2003, the Federal Employee Protection of Disclosures Act of 2003, 2004, and 2005, the USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005, and the Civil Liberties Restoration Act of 2005, are appropriate for release without excision and copies are enclosed. You will note that some this material has been excised pursuant to Exemption 1 of the FOIA. Please be advised that those excisions were not applied by this Office as that information was redacted at the time we located the material. For your information, we did not locate views letter pertaining to any of the other legislation listed in your request letter.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. *See* 5 U.S.C. 552(c) (2006 & Supp. IV 2010). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

If you are not satisfied with my response to this request, you may administratively appeal by writing to the Director, Office of Information Policy, United States Department of Justice, Suite 11050, 1425 New York Avenue, NW, Washington, DC 20530-0001, or you may submit an appeal through this Office's eFOIA portal at <http://www.justice.gov/oip/efoia-portal.html>. Your appeal must be received within sixty days from the date of this letter. If you

submit your appeal by mail, both the letter and the envelope should be clearly marked  
“Freedom of Information Act Appeal.”

Sincerely,

A handwritten signature in blue ink, appearing to read "Vanessa R. Brinkmann", with a small "BR" monogram at the end.

Vanessa R. Brinkmann  
Counsel, Initial Request Staff

Enclosures



# Office of the Attorney General

Washington, D. C. 20530

April 9, 1996

The Honorable Henry Hyde  
Chairman  
Committee on the Judiciary  
U.S. House of Representatives  
Washington, D.C. 20515-6216

Dear Mr. Chairman:

I write to provide you and your colleagues on the conference committee with the views of the Department of Justice on S. 735, the terrorism bill. As you know, enactment of tough and effective antiterrorism legislation is among the Administration's highest priorities. The Department looks forward to working with the conference committee in crafting the strongest, most effective and comprehensive bill possible.

As the conference committee begins its work, several fundamental principles and goals should govern its deliberations. First, we must protect American lives without sacrificing cherished American rights and freedoms. Second, we must give law enforcement the tools it needs to do its job. Third, we must ensure that foreign terrorists are barred from this country. Fourth, we must prevent terrorists from raising money in the United States to carry out their crimes.

The President has transmitted two complementary legislative proposals: the "Omnibus Counterterrorism Act of 1995" and the "Antiterrorism Amendments Act of 1995." These proposals address the challenges posed by domestic and international terrorism in a comprehensive fashion. They include the following major provisions:

- Federal criminal jurisdiction for any international terrorist attack in the United States as well as for terrorists who use the United States as a base from which to plan activities overseas.
- An effective means of preventing fundraising in the United States which supports international terrorism overseas.
- A mechanism to deport alien terrorists expeditiously and fairly, but without risking disclosure of national security information.
- Provisions to update law enforcement's ability to use electronic surveillance by: authorizing multi-point

wiretaps to enable law enforcement to move with a terrorist suspect from phone to phone; adding terrorism cases to the list of cases under which temporary emergency wiretaps may be used; and expanding the list of felonies that could be used as the basis for court-ordered surveillance.

- Authority to use the national security letter process to obtain records in terrorism investigations from hotels, motels, common carriers, and storage and rental facilities.
- Implementation of the Plastic Explosives Convention which requires specified chemicals be added to plastic explosives to permit their detection.
- Requirement of inclusion of microscopic taggants in explosives for tracing purposes.
- A source of funding for the Administration's digital telephony initiative.
- A new Federal offense for the knowing possession of stolen explosives; enhanced penalties for transfer of firearms or explosives knowing they will be used in a crime of violence and for terrorist attacks against Federal employees and their families; and extension of the statute of limitations for certain firearms offenses.

Any comprehensive approach to combatting domestic and international terrorism should include effective provisions in each of these critical areas.

Regrettably, however, the bills advanced by the House and Senate fail to address many of the Administration's key proposals in an effective manner. The House bill in its present form has been stripped of a number of the important tools that law enforcement needs to fully fight domestic and international terrorism. In addition, certain provisions in the House and Senate versions, if enacted into law, would actually make it more difficult to combat terrorist activity.

While both bills contain serious flaws, taken together they could provide a foundation upon which to build strong and effective legislation to combat terrorism. Both the House and Senate included some of the proposals advanced by the Administration, in some cases in modified form. Each bill increases assistance to victims, including worthwhile provisions contained in Title X of the Senate bill. The House bill also contains important provisions, based on Administration submissions, that would significantly improve the biological

weapons statute to address advances in bioengineering and related technology and provide the authorization for a Counterterrorism Center to coordinate our efforts to combat terrorism.

To reach the goal of effective, meaningful antiterrorism legislation will require substantial additional work by the conferees on some key issues, as discussed below.

### Fundraising Support for Terrorists

Funds generated in the United States support some of the most dangerous international terrorist organizations, including Hamas and other terrorist groups. To be effective, counterterrorism legislation should include workable means of helping law enforcement put an end to international terrorist fundraising in the United States.

The Administration's proposal authorizes the Federal government to regulate or prohibit any person or organization from raising or providing funds for the use of any foreign organization that the President designates as engaged in terrorism. The proposal also includes a licensing procedure, administered by the Secretary of the Treasury, to protect the activities of legitimate fundraising organizations.

Unfortunately, the Senate bill contains a substantially impaired version of the Administration's proposal and the House bill does not contain any provision for the designation of foreign terrorist groups that benefit from U.S.-based fundraising. This gap in the coverage of the bills can be corrected by amending the Senate bill in three basic ways:

First, the 30-day prior notification requirement must be deleted. This requirement would give terrorist groups and their supporters sufficient time to smuggle assets out of the United States and to set up new fundraising fronts before the prohibition took effect.

Second, the Senate bill provides an unprecedented and unworkable degree of judicial review over a foreign policy decision, thereby affording foreign terrorist organizations unwarranted legal rights. While we support judicial review, it must be along the lines of the provisions contained in Section 611 of the bill reported by the House Judiciary Committee in June 1995, with some modifications. That bill authorized the designation of terrorist organizations by the Secretary of State in conjunction with the Attorney General. This determination would be subject to judicial review under an Administrative Procedure Act (APA) standard.

Some have suggested that the designation should be made by the President, with that designation subject to this APA review.

We oppose subjecting a Presidential decision to such review. Presidential designations in the area of foreign affairs have rarely, if ever, been subject to any such judicial review, and we see no reason why terrorists should be entitled to more expansive judicial review of Presidential foreign policy determinations than law-abiding American citizens.

Third, the Senate bill fails to include a mechanism for designating the agents who are actually raising the funds in the United States on behalf of the foreign terrorist group. Without such a mechanism, there will be no effective means to enforce the legislation and prevent fundraising.

We will be happy to work with you and your staff to craft a comprehensive and meaningful fundraising provision by addressing these issues.

### Terrorism Transcending National Boundaries

To ensure an effective response to terrorism, we need clear Federal criminal jurisdiction over international terrorist attacks in the United States, as well as the ability to reach those terrorists who use the United States as a base from which to plan activities overseas. Current Federal law does not cover all acts of international terrorism, even where the terrorist acts on instructions from overseas, unless certain narrow statutory bases for jurisdiction are present. For example, certain statutes require that the victims of an attack be government employees or that the building bombed by a terrorist group be an instrument of commerce. Thus the perpetrators of a violent act may do so as part of a terrorist plot, but could not be tried federally for lack of appropriate jurisdiction.

Accordingly, the Administration's proposal creates a new offense for acts of terrorism that transcend national boundaries. The provision is aimed at terrorist acts that take place within the United States, but which are planned or instigated from outside the United States. It does not cover criminal acts of domestic terrorism which are not connected to overseas sources.

The Senate bill essentially encompasses the Administration's original proposal in an effective manner by requiring the Attorney General to certify that the criminal activity transcended national boundaries and was done to coerce or retaliate against a government. This certification is similar to one in existing law (18 U.S.C. §2332(d)), requiring certification that specified criminal acts were "intended to coerce, intimidate, or retaliate against a government or a civilian population."

In contrast, the House version is wholly ineffective: among other things, it limits the coverage of its provision to existing

Federal offenses. Additionally, it would transform the jurisdictional prerequisite -- "transcending national boundaries" -- from a fact to be certified by the Attorney General into an element of the offense. In many cases, this would be extremely difficult to prove beyond a reasonable doubt without disclosing highly classified information.

### Electronic Surveillance

While advances in communications technology have brought the world closer together, they also make it more difficult for law enforcement to keep up with terrorists. To help combat terrorism, the Administration proposed providing law enforcement with the ability to deal effectively with the changes in modern technology that help terrorists avoid detection, while preserving the important privacy protections for electronic surveillance under existing Federal law. These provisions include: authorizing multi-point wiretaps to enable law enforcement to move with a terrorist suspect as he switches from phone to phone; emergency wiretap authority for terrorism cases; applying the same standard in national security cases as is currently used in routine criminal cases for "pen registers" and "trap and trace" devices; and an expanded list of felonies that could be used as the basis for court-ordered surveillance.

Under current law for multi-point wiretaps, law enforcement must show that the targeted individual is changing telephones for the purpose of thwarting surveillance. Establishing an intent to evade surveillance frequently is extremely difficult: criminals may switch phones to pirate cellular service, and may also have reasons for moving from location to location that appear legitimate. The Administration proposal would remove this needless impediment to the issuance of multi-point wiretaps and would more closely align the legal standard for obtaining multi-point wiretaps with the standard for interception of oral, face-to-face conversations, where the government need only show that it would be impractical to specify in advance the place the subject's communications will be intercepted.

In addition, we believe that the Foreign Intelligence Surveillance Court should be authorized to permit pen registers and trap and trace devices in international and domestic terrorism and foreign counterintelligence cases, based on the same standard that exists in criminal cases.

Similarly, emergency wiretap authority is currently available to the Attorney General in cases involving: organized crime, immediate danger of death or serious injury, and conspiracies threatening national security. Such authority is available only for 48 hours and is then subject to judicial review. If a court subsequently finds the emergency authority to have been invoked improperly, no evidence obtained pursuant to



the emergency wiretap is admissible in court. The Administration proposed granting similar authority in terrorism investigations. This expeditious authority may be critical to investigative efforts focused on preventing a terrorist act or identifying the individuals responsible for an act. Given the serious threat posed to our national security by terrorism, it is essential that this emergency authority be extended to these cases.

#### Common Carrier/Hotel Records

The Senate bill contains a provision that requires the Federal Bureau of Investigation to obtain a court order before it may have access to the records of common carriers, hotels, storage facilities, and vehicle rental facilities in foreign counterintelligence investigations, including international and domestic terrorism cases. The House deleted a similar court order provision during the floor debate on the bill. These same records currently may be obtained by the FBI without a court order in the most routine criminal investigations. Giving the FBI similar access to such records here, as requested in the Administration's original proposal, will provide important means of combatting international and domestic terrorism.

The Senate provision as currently drafted, however, raises very serious concerns. Requiring court orders, as the Senate provision does, in the context of foreign counterintelligence cases could risk the disclosure of sensitive foreign counterterrorism investigations. For that reason, this provision will be of no practical use in foreign intelligence and terrorism cases.

#### Alien Removal and Exclusion

The Administration's counterterrorism bills provide an effective and fair procedure for removing terrorists in a manner that does not jeopardize sensitive law enforcement procedures and intelligence information. Although the Constitution's confrontation requirements have never applied to these civil proceedings, under existing immigration law, aliens in deportation proceedings generally are provided with a "reasonable opportunity" to examine the evidence against them. In the absence of clear limitations, however, this purely statutory confrontation right has led to broad claims for discovery of classified information and extensive discovery into intelligence community files. As a result, the Immigration and Naturalization Service often is unable to proceed with a terrorist deportation case unless the Federal Bureau of Investigation can declassify a substantial part of its investigation for use in open court. This restriction compromises ongoing investigations, endangering American lives.

The Senate bill establishes special procedures for alien removal cases that involve classified evidence. These special procedures provide aliens with substantial protections not available to other aliens in conventional deportation proceedings. These include: trial by an independent Article III judge, representation by counsel at government expense, and mandatory certification by the Attorney General or Deputy Attorney General before the proceedings can be instituted.

The Senate bill also contains needed substantive changes to existing terrorism exclusion and deportation provisions that are similar to the Administration proposals. The Senate bill, however, creates a serious problem for our counterterrorism efforts. The bill bars the exclusion or deportation of aliens who provide material support to terrorists, unless the alien can be proven to know the terrorist's future plans. This is a rollback of existing law that effectively guts immigration enforcement over terrorist aliens. Current law requires the removal of aliens who provide material support to terrorist organizations that they know or have known to have committed terrorist acts. The Senate provision, by contrast, permits an alien to provide material support to Hamas literally an hour after one of its suicide bombers blows up a bus, as long as the alien cannot be proven to know Hamas's attack plans for tomorrow. Few terrorists may have that information, and proving that they do will be almost impossible. Similarly, this provision deletes "reasonably should know" from the existing intent standard, and requires that the government prove actual knowledge on the part of the alien, a much more difficult and unnecessary burden.

The House bill establishes procedures for the expedited exclusion of arriving aliens for having presented fraudulent documents or no documents for admission. Specifically, it authorizes the Attorney General to order an alien excluded and deported without opportunity for an immigration judge hearing and without any further administrative review. Only limited judicial review would be available. An exception from expedited exclusion would be provided for aliens who demonstrate a credible fear of persecution upon return to their country. The Senate bill does not include an expedited exclusion provision.

These expedited procedures are an important addition to this legislation. The Department recommends some revisions to the House bill provisions to bring them closer to the flexible and effective exclusion procedures contained in the immigration bill passed by the House as H.R. 2202.

#### Closed Circuit Television Coverage of Oklahoma City Case

The House bill contains a provision to require the closed circuit televising of proceedings, such as the Oklahoma City bombing trial, in which the venue of the trial is changed to a

distant location. This provision, as presently drafted, prohibits the use of appropriated funds to pay for the cost of closed circuit transmission of the proceedings. Instead, such transmission would be dependent on private donations to the Administrative Office of the U.S. Courts. If the conference committee adopts such a provision, the Department strongly urges that it include authorization for its costs from appropriated funds, like any other cost of a trial, in order to ensure control over the transmission so that it is not used in a manner that may jeopardize the case.

The Department has also pursued other means of ensuring that the victims of the Oklahoma City bombing can exercise their right to view court proceedings. In addition to the \$200,000 that the Attorney General has made available through the Office of Victims of Crime (OVC) to assist survivors and loved ones who wish to attend the trial in Denver, the Department has transmitted to the Congress a proposed amendment authorizing OVC to set aside up to \$500,000 to provide travel and lodging funds, and for related assistance. The Department urges the conferees to adopt this proposed authorization.

#### Commission to Investigate Federal Law Enforcement

The House bill includes a provision, adopted during floor debate, to create a new Washington-based commission, which would be charged with investigating Federal law enforcement agencies. The establishment of a commission to investigate Federal law enforcement agencies could be damaging to strong and effective law enforcement and is, at best, redundant and unnecessary. Congress has more than sufficient authority to oversee the activities of Federal law enforcement agencies, and exercises that authority vigorously. The commission's virtually unbridled authority could be used, intentionally or otherwise, to thwart on-going criminal investigations. Finally, the commission would divert precious resources from law enforcement agencies' efforts to combat terrorism and other high-priority criminal investigations. This commission treads directly on the historic oversight function of the Congress as well as the law enforcement duties and responsibilities of the Executive Branch.

#### Habeas Corpus Reform

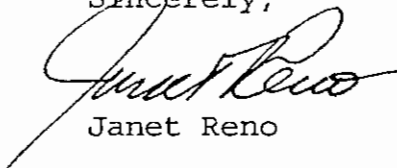
The Administration is committed to any reform that would assure dramatically swifter and more efficient resolution of criminal cases while at the same time preserving the historic right to meaningful Federal review. The Administration hopes to work with the conferees to achieve these goals.

Miscellaneous Provisions

There are a number of additional areas where the Department would suggest substantive changes or minor and technical amendments to miscellaneous provisions to be considered by the conferees. We would be happy to provide you with our suggestions for these proposals at any time.

I appreciate this opportunity to provide the views of the Department of Justice to the conference committee for the terrorism bill. I understand that Secretary of State Christopher and Secretary of the Treasury Rubin will independently share with you their views on this pending legislation, views in which I concur. The Administration is committed to working with the Congress to provide tough and effective new tools to combat domestic and international terrorism and the Department of Justice stands ready to assist the conferees in crafting a meaningful, comprehensive antiterrorism bill.

Sincerely,

A handwritten signature in cursive script, appearing to read "Janet Reno", written in dark ink.

Janet Reno

cc: The Honorable John Conyers, Jr.  
The Honorable Bill McCollum  
The Honorable Steven Schiff  
The Honorable Steve Buyer  
The Honorable Bob Barr  
The Honorable Charles E. Schumer  
The Honorable Howard L. Berman



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

June 14, 1996

The Honorable Stephen Horn  
Chairman, Subcommittee on Government  
Management, Information and Technology  
Committee on Government Reform and Oversight  
U.S. House of Representatives  
Washington, D.C. 20515

Dear Mr. Chairman:

This letter responds to your letter of May 30, 1996, to the Attorney General requesting the views of the Justice Department on H.R. 1281, "The War Crimes Disclosure Act," and S. 1090, "The Electronic Freedom of Information Improvement Act." This letter presents the Department's views on H.R. 1281.

Please note at the outset that the Department strongly supports the goal of informing the public about the horrors of the Holocaust. We believe that disclosing information about those atrocities is in the best interest of the nation and will ensure that the world never forgets the crimes committed. Moreover, the Attorney General is deeply devoted to bringing the perpetrators to justice.

It is precisely because of this devotion that the Department would like to bring to your attention several concerns that we have with the legislation as drafted. We would be happy, of course, to work with you and your colleagues to modify the legislation ensuring that information is disseminated while at the same time ensuring that the Department has the requisite tools to prosecute those involved with Nazi war crimes.

H.R. 1281, "The War Crimes Disclosure Act," would amend the Freedom of Information Act ("FOIA"), 5 U.S.C. §552, to require, with certain exceptions, the disclosure of information regarding individuals who committed Nazi war crimes between December 11, 1941 and May 8, 1945. The bill would accomplish this by taking this information outside the exemptions to the FOIA set forth at 5 U.S.C. 552(b) so disclosure would be required. We fully support declassifying and releasing information pertaining to Nazi war crimes at an appropriate time. However, as drafted, H.R. 1281 would have significant consequences that we are certain its supporters did not intend.

The Attorney General has designated the Office of Special Investigations ("OSI") as the sole office charged with prosecuting Nazi war criminals in the United States and enforcing Public Law No. 95-549, 92 Stat. 2065, sections 101-105 (1978), commonly known as the "Holtzman Amendment" to the Immigration and Nationality Act. The Holtzman Amendment renders excludable or deportable aliens who participated in Nazi persecution. It is the Department of Justice and primarily OSI that would be most affected by H.R. 1281.

Pursuant to H.R. 1281, OSI would be required to disclose case strategy documents which ordinarily would be protected by attorney work product and attorney-client privileges. Because the FOIA requires disclosure to anyone who requests information, H.R. 1281 could provide an enormous advantage to Nazi persecutors by disclosing the Government's investigation and litigation strategies prior to the questioning of persons properly excludable. Similarly, H.R. 1281 would provide information about and insight into the Government's files to persons properly expelled from the United States who seek to attack judgments, orders of deportation, and consent agreements collaterally.

Because H.R. 1281 would include within its coverage, information having nothing to do with the commission of Nazi war crimes, the Department is concerned that the bill is overbroad. Under Section 2(a)(2), the bill covers "any matter that relates to any individual who is potentially excludable from the United States" as a Nazi war criminal, regardless of whether the "matter" relates to the commission of Nazi war crimes (emphasis added). Thus, for example, if an individual were excludable as a Nazi war criminal and also were the subject of an FBI investigation relating to espionage or terrorism, then under the bill, classified information pertaining to that espionage or terrorism investigation would be swept out of the FOIA exemptions at 5 U.S.C. 552(b) and swept into the very different provisions of the bill.

Furthermore, the Department is concerned that H.R. 1281 would burden OSI's declining resources substantially by requiring the review, segregation, redaction, copying, and production of huge quantities of documents. Given unchanged resource levels, these activities would require an enormous investment of the current staff's time when time is the greatest enemy of OSI's prosecution effort. Virtually all of the subjects and key witnesses in these cases are now more than 70 years of age. Enactment of this legislation effectively would mean that some Nazi persecutors might never be prosecuted since key OSI personnel would be diverted from their crucial investigatory and prosecutorial roles to the dissemination of documents. H.R. 1281 would fundamentally disable the very effort -- disclosure of information to the public about those who assisted in Nazi-sponsored persecution -- which the bill seeks to enhance and which the Department supports.

Unwarranted invasions of individual privacy rights could also be affected by the bill's scope because H.R. 1281 provides access to individuals listed on the Watchlist. The Watchlist is a collection of names of tens of thousands of individuals who are suspected of having participated in persecution during World War II. The purpose of the Watchlist is to afford the government the opportunity to investigate the individuals further should they attempt to enter the United States. In the vast majority of cases, the watchlisting of an individual signifies only that there is a "reasonable basis to suspect" involvement in Nazi persecution, usually because the individual is believed to have served in a certain unit or organization. Because the threshold required for entering someone on the Watchlist is minimal, certain persons listed could actually establish their innocence of involvement in Nazi persecution. Thus, subjecting all those watchlisted to disclosure might unfairly tarnish or ruin their reputations. OSI has already had the experience, on a number of occasions, of watchlisted individuals (some of whom were, in fact, victims of Nazi persecution) establishing that they were the subject of mistaken identity or were otherwise almost certainly innocent of committing Nazi-sponsored acts of persecution. Therefore, the Department is concerned that Section 2(a)(2) of the bill would not protect the privacy interests of these individuals.

Section 2(a)(2) provides for disclosure of classified information pertaining to Nazi war criminals unless "there is clear and convincing evidence that the threat to national security, military defense, intelligence operations, or the conduct of foreign relations of the United States [presented by disclosure] outweighs the public interest in the disclosure." By amending the FOIA in this manner, the bill would permit the courts to review decisions by Federal agencies not to declassify information pertaining to Nazi war criminals under the bill's balancing analysis, without limiting the ability of the courts to look behind the Executive's national security determinations. The judicial examination of the Executive's national security determinations potentially raises separation of powers concerns.

Moreover, we believe that H.R. 1281 would hinder the Department's efforts to denaturalize, deport and exclude Nazi persecutors significantly. It would give those who seek to obstruct this program a new and potentially powerful weapon for impeding or even disabling it. It could unfairly ruin the reputations of innocent persons. It could set a dangerous precedent for jettisoning the FOIA scheme for other categories of law enforcement documents. Ironically, passage of the bill would undermine its very purpose: exposing the horrors of the Holocaust.

In our view, Executive Order No. 12958 (issued in April 1995), governing the standards for classifying and declassifying information, moves significantly in the direction of striking the

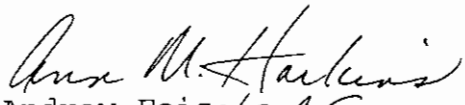
appropriate balance in cases covered by the bill. Specifically, the Order establishes a framework to declassify information if "the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure." This language strikes the appropriate balance for those instances in which the prospect of declassifying implicates both a public interest militating in favor of declassifying and national security-related concerns militating in favor of classifying. In such situations, the Order allows an agency to declassify information otherwise meeting the standards for declassification where the public's interest in disclosure outweighs the need to protect the information.

Additionally, President Clinton issued a statement on October 4, 1993 supporting the release of information under the FOIA. This Department supports the principles articulated in President Clinton's announcement. Moreover, in response to the President's statement, the Attorney General issued new guidelines restricting the Department's ability to withhold information based upon an existing legal basis. Instead, the Attorney General said that "it shall be the policy of the U.S. Department of Justice to defend the assertion of a FOIA exemption only in those cases where the agency reasonably foresees that disclosure would be harmful to an interest protected by that exemption." This policy, together with Executive Order No. 12958, would, in effect, provide for the release of information when appropriate.

The Office of Management and Budget has advised this Department that there is no objection to the submission of this report from the standpoint of the Administration's program.

I look forward to working with you as we move forward in the legislative process and please let me know if I may be of further assistance in this matter.

Sincerely,

  
Andrew Fois *for AF*  
Assistant Attorney General

cc: Honorable Carolyn Maloney  
Ranking Minority Member  
Subcommittee on Government  
Management, Information and  
Technology  
Committee on Government Reform and Oversight





U.S. Department of Justice

Office of Legislative Affairs

---

Washington, D.C. 20530

September 24, 1998

The Honorable Richard C. Shelby  
Chairman  
Select Committee on Intelligence  
United States Senate  
Washington, D.C. 20510

Dear Mr. Chairman:

This letter sets forth the views of the Department of Justice on S. 712, "The Government Secrecy Act," as reported by the Senate Committee on Governmental Affairs. The Department strongly supports the bill's goal of improving the management and reducing the costs of the Government's classification and declassification program. However, as discussed below, we have serious objections to provisions of S. 712 that could impinge upon the President's authority and flexibility to manage the classification program. Taken as a whole, the bill raises significant separation of powers concerns. Legislation in this area should be limited, given the great deference traditionally afforded to the President's authority to protect national security information, which derives from his constitutional responsibilities in the areas of national defense and foreign affairs.

1. Effects on Judicial Review

We are deeply concerned about the implications that the bill's public interest balancing test could have for judicial review of Executive branch national security decisions. Under this legislation, information could not be originally classified (nor could previously classified information continue to be protected) unless "the harm to national security that might reasonably be expected from disclosure . . . outweighs the public interest in disclosure." Section 2(c)(1). In assessing harm to national security, Executive branch officials would be required to consider whether the information fell within one of several specified categories (section 2(c)(3)(A)), and on the other side of the balance, they would have to consider whether the information fell within any of several specified categories where the public might benefit from disclosure (section 2(c)(3)(B)). Where there is "significant doubt" about whether this standard is satisfied, the information shall not be classified (or, if classified previously, it shall be declassified). Section 2(c)(2). A separate provision apparently requires "a

demonstrable need" for information to be classified. Section 2(a); see also § 2(d)(4)(D)(i) (requiring "extraordinary circumstances" for continued classification beyond specified dates).

This balancing test is a drastic change from current classification policy, as established by Executive Order 12958. Under this order, there is no balancing test for original classification decisions. During declassification reviews, officials may, in "exceptional cases" and "as an exercise of discretion," declassify information that otherwise would remain classified if they determine that "the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure." Executive Order 12958 § 3.2(b). This discretionary authority does not "amplify or modify the substantive criteria" for classification or "create any substantive or procedural rights subject to judicial review." Id.

In contrast, legislating a mandatory balancing test for all classification decisions as a substantive classification requirement (as opposed to an exceptional discretionary declassification consideration) not only would deprive the President of flexibility to respond to particular circumstances that may not fit the rigid criteria defined by Congress, but it also could transform the nature of judicial review of classification and declassification decisions in Freedom of Information Act (FOIA) litigation. The specific features of the balancing test provision are substantive criteria for classification and therefore decisions under the balancing test would be subject to judicial review because the bill permits review under FOIA of substantive classification decisions (section 6(b)). Courts generally have recognized the constitutional authority, responsibility, and institutional expertise of the Executive branch in the national security area and accordingly have deferred to its classification decisions. However, under the bill's mandatory balancing test, there is a risk that, over the Executive branch's objection, the Judiciary might reconsider its traditional deference to classification decisions now that those decisions would require a finding that the "public interest" in disclosure (as defined in the bill) is overcome by the need to protect information. Courts now properly defer to the judgment and discretion involved in Executive branch determinations that disclosure of information reasonably could be expected to damage the national security. Given the specificity of the factors on each side of the balance that this bill spells out, courts might conclude that there is "law to apply" (see *Citizens to Preserve Overton Park v. Volpe*, 401 U.S. 402, 410 (1971)) and undertake review with little or no deference to the Executive branch's authority and expertise.

We are concerned that no matter what the bill or its legislative history might say about intending that there be no change in judicial deference, for the reasons stated above the courts might reject the arguments the Executive branch would make to them on this point and replace the deference now afforded classification decisions in FOIA litigation with considerably closer judicial scrutiny. Accordingly, the balancing test raises substantial separation of powers concerns because it would encourage the courts to take action that could transgress upon the President's constitutional authority.

In addition to the balancing test, the bill's default rule in favor of nonclassification or declassification when there is "significant doubt" whether disclosure "might reasonably be expected" to harm national security or whether such harm would be outweighed by the public interest could lead to judicial inquiry into whether a decisionmaker had significant doubt. Such proceedings would intrude on highly discretionary judgments of experts. Moreover, the "significant doubt" provision at section 2(c)(2) suggests a different standard from "demonstrable harm" under section 2(a), which would lead to litigation over how these provisions should be applied together. Yet another provision, requiring that older information can be kept classified only in "extraordinary circumstances" (section 2(d)(4)(D)(i)), also could be the subject of litigation over how it should apply to information sought by a FOIA request.

Other provisions of the bill could affect judicial review. The requirement for a written, "detailed justification" for each classification decision (section 2(c)(4)) would impose considerable administrative burdens and consume resources that agencies otherwise could devote to their core missions, while creating justifications that could be more sensitive than the underlying records. This provision also could lead to judicial mandates to disclose sensitive information in FOIA litigation if the court found a failure to comply with this provision (e.g., because the justification was deemed insufficiently detailed in its application of the statutory standards and criteria). The provisions requiring certification to the President and the concurrence of the Director of the proposed Office of National Classification and Declassification Oversight in order to retain classification beyond specified dates (section 2(d)(3)-(4)) could present comparable practical burdens and litigation risks.

## 2. Classification Criteria

Beyond these separation of powers concerns about judicial review, we believe that the bill's criteria and standards for classification would unduly restrict the ability of the Executive branch to protect sensitive information, especially in original classification decisions. The criteria and standards are significantly narrower than those in the current executive order

on classification, Executive Order 12958. The categories of information eligible for original classification under Executive Order 12958 (provided that the damage-to-national-security requirement of section 1.2(a)(4) also is met) are considerably broader than the categories stated in section 2(c)(3)(A) of the bill. The bill's classification categories are taken verbatim from section 3.4(b) of Executive Order 12958, which describes information that, under the Executive Order, may be exempt from declassification after 25 years. Because the information is older, the Executive Order's categories for continued classification after 25 years are quite narrow. However, this bill would require an official making an original classification decision to consider whether current information falls into these same narrow categories.

Imposing declassification criteria for very old information onto original classification determinations would be a significant and unwarranted departure from current policy. The Executive Order properly recognizes that information about today's intelligence operations, diplomatic initiatives or weapons systems is categorically more sensitive than information on these subjects from many years ago. Accordingly, the classification categories and standards set out in section 3.4(b) may be appropriate for continued classification of 25-year-old information, but not for original classification of current information. Applying these categories to original classification within the framework of the new balancing test is likely to lead to confusion, insufficient protection, or both. These problems would be exacerbated by the fact that the President could not modify legislatively-established categories and standards to respond to changed or changing circumstances in an appropriate and timely manner.

### 3. Proposed Review Board

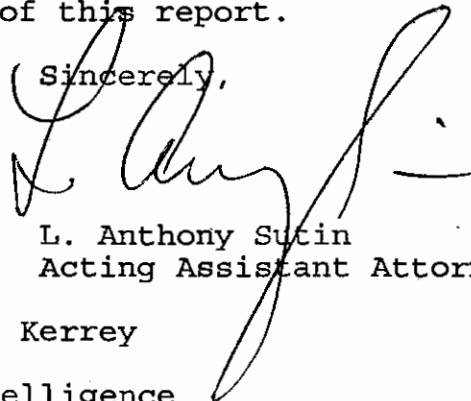
Finally, establishment of the proposed Classification and Declassification Review Board ("Review Board") could further erode the President's constitutional authority. The bill requires that the Board be composed solely of private citizens, whose lack of current institutional responsibility and experience may undercut their ability to make fully informed declassification decisions. This prohibition on appointing Government employees with current institutional expertise is not only unwise as a matter of national security policy, it also may impermissibly limit the President's exercise of his appointment authority under the Constitution. See Civil Service Commission, 13 Op. Att'y Gen. 516, 520 (1871) (Constitution requires that when Congress creates an office, it must leave sufficient "scope for the judgment and will of the person or body in whom the Constitution vests the power of appointment").

Moreover, it is difficult to envision in practical terms exactly what the Review Board would contribute to the appeal process. Given the designedly disclosure-oriented composition of the Review Board, it would be extremely rare for the Review Board to overturn a decision by the Director of the Oversight Office that particular information should be declassified. Thus, in appeals under section 4(c)(1)-(2), the Review Board would provide a second, superfluous review within the Executive Office of the President, without affecting ultimate outcomes.

Appeals by requesters of mandatory declassification reviews, which would come to the Review Board under section 4(c)(3), are now decided by the Interagency Security Classification Appeals Panel (ISCAP). See Executive Order 12958 §§ 3.6(d), 5.4(b)(3). The Panel is composed of representatives appointed by the Attorney General, the Secretaries of State and Defense, the Director of Central Intelligence, the National Security Adviser, and the Archivist of the United States, with a chair appointed by the President. Since its first meeting in April 1996, ISCAP has declassified in full 61.5% of the documents on which it has acted and has declassified substantial portions of an additional 23%. This record demonstrates that searching appellate review of mandatory declassification requests is already available. A statutory Review Board is not needed to perform this function.

Thank you for the opportunity to present our views. Please do not hesitate to call upon us if we may be of further assistance. The Office of Management and Budget advises that, from the standpoint of the Administration's program, it has no objection to the submission of this report.

Sincerely,



L. Anthony Sutin  
Acting Assistant Attorney General

cc: The Honorable J. Robert Kerrey  
Vice Chairman  
Select Committee on Intelligence

The Honorable Fred Thompson  
Chairman  
Committee on Government Affairs

The Honorable John Glenn  
Ranking Minority Member  
Committee on Government Affairs



U.S. Department of Justice

Office of Legislative Affairs

---

Washington, D.C. 20530

May 17, 2000

The Honorable Arlen Specter  
United States Senate  
Washington, D.C. 20510

Dear Senator Specter:

This letter responds to your May 4, 2000, letter to Frances Fragos Townsend, the Department's Counsel for Intelligence Policy, in which you requested the views of the Justice Department on the current version of S. 2089, the "Counterintelligence Reform Act of 2000." S. 2089 would, among other things, amend the Foreign Intelligence Surveillance Act of 1978 ("FISA").

We appreciate that concerns the Department had expressed about prior versions of this legislation have now been addressed. Specifically, we note that the special "probable cause" standard and the proposed change to FISA's definition of "agent of a foreign power" (both included in a prior draft) have been replaced by new provisions set forth in sections 2, 3(c), and 4(c) of the bill.

Section 2 of the bill would confirm and emphasize that an individual is an "agent of a foreign power" under FISA when the individual provides classified information to and for the use or benefit of a foreign power in a manner that involves or may involve a violation of Federal criminal law. This provision correctly recognizes that those who share classified information with a foreign power in a way that is or may be inconsistent with Federal criminal law may be the subject of surveillance under FISA. At the same time, the provision does not deem an individual who shares classified information with a foreign government in an authorized manner (*i.e.*, in a manner consistent with Federal criminal law) an agent of a foreign power solely on the basis of his lawful, authorized activity.

We note that under FISA in its current form, the unauthorized sharing of intelligence with a foreign power already

may render an individual an agent of a foreign power. We have no objection to section 2, provided that it is accompanied by committee report language pointing out that the provision merely confirms and emphasizes the Government's preexisting authority under FISA and in no way limits the authority already conferred by the statute.

We also have no objection to sections 3(c) and 4(c) of the bill. Under these provisions, the Foreign Intelligence Surveillance Court would be authorized, but not required, to "consider past activities of the target" when determining whether or not probable cause existed for issuance of certain orders under FISA. We note that here, too, under FISA in its current form, the Court already may consider such past activities.

We also appreciate the modifications that have been made to sections 3(b) and 4(b) of the legislation. The prior versions of these provisions called for a series of steps (written requests, written notices responding to those requests, and supervision of written changes to certain kinds of FISA applications) to be personally taken by the Attorney General, the Director of the Federal Bureau of Investigation, the Secretary of Defense, the Secretary of State, and the Director of Central Intelligence. As modified, sections 3(b) and 4(b) would -- appropriately -- permit these senior officials to delegate the responsibilities that the provisions would establish.

We appreciate the legislation's support for the Department's national security role, as set forth in sections 7(a) and (b) of the bill, which, among other things, would authorize additional funding for the Department's Office of Intelligence Policy and Review.<sup>1</sup> As the text of section 7(a) properly recognizes, the Office of Intelligence Policy and Review needs these additional resources in order to help meet the increased personnel demands associated with that office's policy and operational responsibilities with respect to counterterrorism, counterintelligence, and other national security matters.

Under section 7(c) of the bill, the Attorney General would be required to report to the Committees on the Judiciary of the

---

<sup>1</sup>Page 14, line 17 of the bill should be modified by moving "and" from its current location and placing it immediately after "Policy."

Senate and the House of Representatives, within 120 days, on "actions that have been or will be taken by the Department" to centralize the handling of national security issues.

Instead of a formal reporting requirement, we respectfully submit that an appropriate alternative would be for the Department to brief the Committees on the important issues implicated by section 7(c), so that approaches may be developed about how to improve the manner in which the Department conducts its national security missions -- approaches that are agreeable both to the Committees and the Attorney General.

We also respectfully recommend that a clarification be considered to section 8(a). This provision would authorize additional appropriations for activities of the Criminal Division's Computer Crime and Intellectual Property Section, the Federal Bureau of Investigation, and the Office of Justice Programs' Bureau of Justice Assistance to help meet the increasing demand for training, investigative and prosecutorial resources.<sup>2</sup> However, it is not clear that these funds would be available for use by individual United States Attorneys' offices, to allow them to add additional prosecutorial resources outside of headquarters components. We therefore recommend that the United States Attorneys be included in the list of offices enumerated in this section.

Section 8(c) would add to existing reporting obligations appearing at 18 U.S.C. § 2320(f)(1) through (4) the requirement that the Department report on "[t]he number of cases and offenses committed involving the criminal use of the Internet." While we are appreciative of the heightened priority Congress has afforded these matters and we are taking steps to raise the priority of criminal intellectual property investigations and prosecutions nationwide, we are concerned that the creation of the mechanisms

---

<sup>2</sup>We suggest that the bill's references to the Computer Crime and Intellectual Property Section and the Bureau of Justice Assistance (page 15, line 25 through page 16, line 2) be revised to refer, respectively, to the Criminal Division and the Office of Justice Programs (the larger components in which the section and the bureau are located). Alternatively, we suggest that the bill be revised to insert "of the Criminal Division" on page 16, line 1, immediately after "Section," and to insert "of the Office of Justice Programs" on page 16, line 2, immediately after "Assistance."



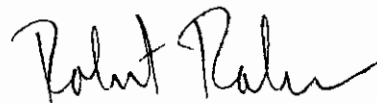
required to substantively evaluate and track these cases might detract from the resources available to investigate and prosecute them. Given the challenges associated with producing more comprehensive statistics on Internet misconduct generally, we also question whether placing additional reporting burdens on the Department in this subject-matter specific manner would be helpful.

We would prefer to work with Congress to achieve, in the longer term, more effective ways of assessing the harm done by a broader range of misconduct involving the use of computers and computer-based technology.

Finally, upon further study of the legislation, some components of the Department have raised concerns regarding section 5's requirement that regulations be promulgated regarding disclosure for law enforcement purposes of information acquired under FISA. This matter is currently under review in the Department. To the extent that further clarification regarding such disclosures is required it is not apparent that regulations are the appropriate vehicle for doing so. Indeed, in the view of some components of the Department, such regulations are likely to complicate espionage or terrorism prosecutions by engendering litigation over whether the regulations afford defendants procedural or substantive rights. It is thus the view of some components of the Department that the better approach is for the Department to keep the Committees informed of the Department's own review of the issue of disclosure and the conclusions reached by that review.

Thank you for the opportunity to present our views. Please do not hesitate to call upon us if we may be of additional assistance. The Office of Management and Budget has advised us that from the standpoint of the Administration's program, there is no objection to the submission of this letter.

Sincerely,

A handwritten signature in dark ink, appearing to read "Robert Raben". The signature is fluid and cursive, with the first name "Robert" and last name "Raben" clearly distinguishable.

Robert Raben  
Assistant Attorney General



U.S. Department of Justice

Office of Legislative Affairs

---

Washington, D.C. 20530

July 17, 2000

The Honorable Richard C. Shelby  
Chairman  
Select Committee on Intelligence  
United States Senate  
Washington, D.C. 20510

Dear Mr. Chairman:

This letter presents the views of the Department of Justice on S. 2089, the "Counterintelligence Reform Act of 2000," as reported by the Senate Committee on the Judiciary and referred to the Committee on Intelligence. The Department commented on an earlier version of this bill in our letter of May 17, 2000. We support much of the current version of the legislation and favor the bill's passage subject to the following concerns.

**S. 2089 as Reported by the Committee on the Judiciary**

Section 4 requires that regulations be promulgated regarding disclosure for law enforcement purposes of information acquired under the Foreign Intelligence Surveillance Act of 1978 ("FISA"). To the extent that further clarification regarding such disclosures is necessary, it is not apparent that regulations are the appropriate vehicle for doing so. Such regulations are likely to complicate espionage or terrorism prosecutions by engendering litigation over whether the regulations afford defendants procedural or substantive rights. The Department would be pleased to keep the appropriate Congressional committees informed of the Department's own review of the issue of disclosure and the conclusions reached by that review.

Additionally, under section 6(c) of the bill, the Attorney General would be required to report to the Committees on the Judiciary of the Senate and the House of Representatives, within 120 days, on "actions that have been or will be taken by the Department" to centralize the handling of national security issues.

An appropriate alternative to a formal reporting requirement would be for the Department to brief the appropriate Congressional committees on the important issues implicated by section 6(c), so that approaches may be developed about how to improve the manner in which the Department conducts its national security missions -- approaches that are agreeable both to the committees and the Department of Justice.

Finally, section 6(a), page 24, line 1 of the bill, should be modified by moving "and" from its current location and placing it immediately after "Policy."

#### **Amendment Modifying the Classified Information Procedures Act**

We understand that the Committee may consider an amendment to S. 2089 that would modify section 9 of the Classified Information Procedures Act ("CIPA") to establish "certain administrative requirements relating to the prosecution of cases involving classified information." Although broadly worded to cover all cases involving classified information, the amendment plainly is directed toward espionage cases. We strongly oppose this amendment.

First, the amendment does not clearly define the types of cases that its provisions would affect. For example, it would mandate that "victim" agencies<sup>1</sup> in cases "involving classified information" submit to the Attorney General a damage assessment for the case. We note that many Federal criminal cases potentially "involve" classified information.<sup>2</sup>

---

<sup>1</sup>That is, Government agencies that are victimized by espionage.

<sup>2</sup> The revised draft of this amendment does nothing to change our opposition to this proposal. The new draft does not describe with certainty the cases to which it applies. As the new definition of the required damage assessment refers to "information alleged to have been gathered or transmitted in violation of federal law," (f) (2) (A), the section seems aimed at any violation of 18 U.S.C. 793, 794, or 798. Accordingly, it would include in addition to foreign espionage, all unauthorized disclosures of classified information, including media leaks, and other conduct covered by these provisions no matter how de minimus. As the Department has advised the Committee, and as the Attorney General recently testified regarding the proposed

Second, the guidelines issued by the Attorney General pursuant to section 12 of CIPA already provide the guidance necessary to enable prosecutors to assess the nature and importance of classified information involved in Federal criminal cases, including espionage cases. See Attorney General Guidelines For Prosecutions Involving Classified Information, §b (1981).

Third, the amendment would require that prosecutors obtain and review a written damage assessment before making a final decision on whether to take a case to trial or to offer a plea bargain. As described below, this requirement not only would provide a potentially discoverable road map to the case, but could restrict prosecutors in developing trial strategies.

In espionage cases, one of the key elements the Government must prove is that the compromise of classified information relates to the national defense and could be used to injure the United States or benefit a foreign country. Gorin v. U.S., 312 U.S. 19 (1941); U.S. v. Heine, 151 F.2d 813 (2d Cir. 1945), cert. denied, 328 U.S. 833 (1946). Since a damage assessment would address these issues, there is a possibility that it would be discoverable, providing a road map to the defense on the Government's likely proof with respect to this element. Certainly the fact that an assessment is statutorily required would lead the defense in every case to litigate its discoverability. Moreover, the fact that the document might be discoverable could lead the agency whose information has been disclosed to dilute its findings in order to protect against the disclosure to the defense of sensitive classified information, distorting the seriousness of the defendant's activities. Finally, the requirement likely would lock the Government into using the person who prepared the assessment as a witness on the issue of national defense relatedness and damage, even if another person would be a more effective trial witness. For all of these reasons, it has been our practice not to obtain a written damage assessment in espionage cases until after trial or conviction.<sup>3</sup>

---

legislation on unauthorized disclosure of classified information, we are concerned that that legislation as drafted would criminalize inadvertent disclosures.

<sup>3</sup> Nor is our view changed by the provision in the revised amendment that would allow the Assistant Attorney General to waive the preparation of the otherwise mandatory damage

Fourth, the amendment would require the prosecution team to brief the head of the victim agency or that person's designee on the status of the case on a recurring basis; record, for inclusion in the case file, any and all objections by the victim agency to the proposed handling of the case by the Attorney General; and require the Department of Justice's Internal Security Section to reduce to writing key instructions to prosecutors in the field, which instructions would have to be approved by the FBI and the victim agency for clearance before they could be implemented. These rigid requirements also would impede espionage prosecutions, by introducing extensive briefing requirements and burdensome paperwork. In addition, since the determination that a case could result in prosecution is usually made during the investigatory stage, there very well may be grand jury disclosure issues under Rule 6(e) of the Federal Rules of Criminal Procedure arising from the requirement that the agency head be kept "fully and currently informed" of the status of a case. Beyond this, while it has been our practice to brief agency heads generally about espionage investigations and prosecutions that concern their agencies, there may be sound investigative reasons for not doing so, e.g., to prevent leaks during the pendency of an arrest.

Documenting an agency's concerns about the potential discovery, use, and relevance of sensitive, classified information could prove to be a monumental task. But more importantly, it also could create undue pressure on prosecutors

---

assessment upon a written determination that: exigent circumstances necessitate proceeding without one; or that the prosecution is "untenable," or "in conjunction" with the victim agency, that the production of a damage assessment would have an "adverse impact on the outcome of the case." Apart from the obvious ambiguity of the term "untenable," the requirement to have the Assistant Attorney General render such a determination in every case where prosecution is declined is both unproductive and unduly burdensome. That consideration may be given by the drafters to elevating this determination to the Attorney General only makes this provision more problematic. Finally, having the victim agency participate in the determination that prosecution would be adversely impacted by a damage assessment dilutes the authority of the Assistant Attorney General by including agencies in significant litigation decisions when they are unlikely to possess the requisite litigation or prosecutorial expertise.

to satisfy agency concerns, which could delay proceedings and ultimately jeopardize or weaken the Government's case. Further, the creation of a file of complaints about how the Department is handling the case will lead inevitably to discovery requests by espionage defendants for access to a road map to the case and repository of prosecution strategy.

Fifth, the amendment would mandate that key instructions from the Internal Security Section to the United States Attorneys' Offices be reduced to writing and transmitted to the FBI and the victim agency for comment before a final decision is made on the treatment of the case by the United States Attorney. While there are some key instructions in espionage cases that are discussed routinely in advance with either the victim agency, the FBI, or both (proposed dispositions by plea, for example), many are not. As head of the Justice Department, the Attorney General and not the FBI must retain the ultimate authority to manage the Government's litigation.

Thank you for the opportunity to present our views. Please do not hesitate to call upon us if we may be of further assistance. The Office of Management and Budget advises us that from the standpoint of the Administration's program, there is no objection to submission of this letter.

Sincerely,



Robert Raben  
Assistant Attorney General

IDENTICAL LETTER TO BE SENT TO THE HONORABLE RICHARD BRYAN, RANKING MINORITY MEMBER, SELECT COMMITTEE ON INTELLIGENCE; THE HONORABLE ARLEN SPECTER, CHAIRMAN, DEPARTMENT OF JUSTICE OVERSIGHT INVESTIGATION, SUBCOMMITTEE ON ADMINISTRATIVE OVERSIGHT AND THE COURTS, COMMITTEE ON THE JUDICIARY; THE HONORABLE ORRIN G. HATCH, CHAIRMAN, COMMITTEE ON THE JUDICIARY; THE HONORABLE PATRICK J. LEAHY, RANKING MINORITY MEMBER, COMMITTEE ON THE JUDICIARY; THE HONORABLE CHARLES E. GRASSLEY, CHAIRMAN, SUBCOMMITTEE ON ADMINISTRATIVE OVERSIGHT AND THE COURTS, COMMITTEE ON THE JUDICIARY; AND THE HONORABLE ROBERT G. TORRICELLI, RANKING MINORITY MEMBER, SUBCOMMITTEE ON ADMINISTRATIVE OVERSIGHT AND THE COURTS, COMMITTEE ON THE JUDICIARY



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

January 10, 2005

The Honorable Patrick J. Leahy  
Ranking Minority Member  
Committee on the Judiciary  
United States Senate  
Washington, D.C. 20510

Dear Senator Leahy:

This responds to your letter, dated November 8, 2004, to the Attorney General regarding § 2191 of H.R. 10, which proposed amendments to Rule 6 of the Federal Rules of Criminal Procedure affecting the disclosure of federal grand jury information. In substance, these amendments were previously enacted by § 895 of the Homeland Security Act of 2002, Pub. L. 107-296. They have recently been re-enacted by section 6501 of Pub. L. 108-458, the Intelligence Reform and Terrorism Prevention Act of 2004, which was signed by the President on December 17, 2004. Your letter expresses concerns regarding these amendments, and particularly language in the amendments that authorizes contempt sanctions for state and local officials who knowingly disclose federal grand jury information in violation of "guidelines jointly issued by the Attorney General and the Director of National Intelligence pursuant to Rule 6."<sup>1</sup>

We believe that some explanation of the background and purpose of these amendments may alleviate your concerns. The earliest version of these grand jury amendments appeared in S. 1615 of the 107th Congress, which was sponsored by Senator Schumer. The co-sponsors of that bill were Senator Hatch, Senator Clinton, and yourself. The bill generally aimed to broaden the sharing of national security-related information with appropriate state and local officials, including grand jury information, electronic surveillance information, and foreign intelligence information generally.

---

<sup>1</sup> The version in H.R. 10 referred to guidelines jointly issued by the Attorney General and the "Director of Central Intelligence," as a result of incomplete editing that did not fully conform the amendment language to the creation of the office of the Director of National Intelligence and the elimination of the office of the Director of Central Intelligence. The enacted version of the Rule 6 amendments in section 6501 of Pub. L. 108-458 refers consistently to guidelines jointly issued by the Attorney General and the Director of National Intelligence.

The grand jury information sharing provisions in § 2 of S. 1615 provided that state and local officials who receive information pursuant to the broadened information sharing authorization "shall only use that information consistent with such guidelines as the Attorney General shall issue to protect confidentiality." In light of S. 1615's proposed incorporation of this requirement to comply with Attorney General guidelines into Rule 6, and Rule 6's general provision that knowing violations of the Rule may be punished as contempt of court, state and local officials who used federal grand jury information in a manner inconsistent with the contemplated Attorney General guidelines could have been subject to contempt sanctions under the amendments proposed in S. 1615. This is so because a violation of the guidelines would be a violation of the Rule's requirement to comply with the guidelines.

Thus, the original version of the grand jury information sharing amendments – in common with all subsequent versions – would have allowed contempt of court sanctions for violations by state or local officials of guidelines issued by an executive officer (the Attorney General) to protect the confidentiality of federal grand jury information shared with such officials.

We sent you a formal statement of views concerning S. 1615 on April 30, 2002 ("the Letter"). We have enclosed the Letter for your convenience. The letter endorsed the objectives of the bill and many of its specific provisions. Regarding the grand jury information sharing provisions in § 2 of the bill, the Department recommended in part that the authorization of information sharing with state and local officials be more carefully tailored to the types of information that such officials need to carry out their responsibilities, including particularly terrorism threat information. *See Letter, supra*, at 4-9.

The textual suggestions in the Department's views letter carried forward the provision of S. 1615 for compliance with Attorney General guidelines to ensure that state and local officials who receive federal grand jury information will not engage in improper secondary dissemination or other misuse of the information.<sup>2</sup> In addition, the letter included a suggested amendment to Rule 6's contempt provision to refer explicitly to these guidelines. This was merely a clarifying provision, which made explicit a consequence that had been implicit in S. 1615 (see discussion above). The letter explained:

[T]he Department's proposal contains safeguards against the misuse of threat information. It follows Rule 6(e)(3)(C)(i)(IV) in permitting disclosure only for a specified purpose – "preventing or responding to" a threat. It also amends Rule

---

<sup>2</sup> The suggested text in the Department's letter referred to guidelines issued jointly by the Attorney General and the Director of Central Intelligence, rather than to guidelines issued just by the Attorney General, in light of the Director of Central Intelligence's interest in the use made of sensitive national security information.



6(e)(3)(C)(iii) to provide that recipients may use the disclosed information only as necessary in the conduct of their official duties and subject to limits on unauthorized disclosure and guidelines issued by the Attorney General. The use of Attorney General guidelines, which like much of our proposal is derived directly from S. 1615, protects information beyond what was required for disclosures under Rule 6(e)(3)(C)(i)(V) as added by the USA Patriot Act. Finally, subsection (b) of the proposal makes clear that knowing violations of the Attorney General's guidelines, like knowing violations of Rule 6 itself, are subject to punishment as a contempt of court under Rule 6(e)(2).

Letter, *supra*, at 8-9.

The grand jury information sharing provisions, in substantially the version proposed in the Department's letter, were initially passed by the House of Representatives in § 6 of H.R. 4598 on June 6, 2002. During the House Judiciary Committee's consideration of this legislation, the provisions for compliance with guidelines safeguarding the confidentiality of shared information, and for potential contempt sanctions, were pointed to as responsive to concerns about overly broad dissemination or misuse of grand jury information. See H.R. Rep. No. 534, Part I, 107th Cong., 2d Sess. 12 (2002) ("the recipients may only use the disclosed information in the conduct of their official duties as is necessary and they are subject to the restrictions for unauthorized disclosure – including contempt of court"); *id.* at 56-58 (text of Rule 6 amendments); *id.* at 63-64 (remarks of Rep. Green) (noting provision for promulgation of guidelines by the Attorney General and the CIA Director for the use of such information "with which State and local officials must then comply").

Congress thereafter enacted these grand jury information sharing amendments in § 895 of the Homeland Security Act of 2002, Pub. L. 107-296. However, the enacted amendments were inadvertently nullified when a general revision of Fed. R. Crim. P. 6, promulgated at an earlier time by the Supreme Court, became effective shortly after the enactment of the Homeland Security Act.

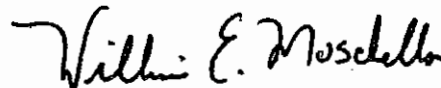
Because of this nullification, re-enactment of these amendments was necessary in § 6501 of Pub. L. 108-458, the Intelligence Reform and Terrorism Prevention Act of 2004. The purpose of the guidelines (and the related contempt sanction provision) in this legislation remains the same as in all earlier versions – to safeguard the confidentiality of federal grand jury information that is shared with non-federal officials. The objectives served thereby include protecting the privacy and reputations of persons to whom grand jury information relates, and preventing the compromise of grand jury investigations. Since the amendments only require non-federal officials who receive grand jury information under Rule 6(e)(3)(D) to use the information consistent with guidelines issued by the Attorney General and the Director of National Intelligence, the possibility of contempt sanctions for violations of these guidelines only applies to such officials.

The Honorable Patrick Leahy  
Page 4

In closing, we would note that there is nothing new about authorizing criminal sanctions for violations of rules issued by executive officials. *See, e.g.*, 21 U.S.C. 821 (Attorney General authorized to promulgate rules and regulations regarding controlled substances); 18 U.S.C. 923 (Attorney General authorized to promulgate regulations regarding licensing of firearms); 18 U.S.C. 2257 (Attorney General authorized to issue regulations regarding recordkeeping in the production of visual depictions of sexually explicit conduct). In each case, the criminal charge may reference the underlying statute together with the particular regulation that was violated. Similarly, an official who breached grand jury secrecy requirements as articulated in guidelines issued by the Attorney General and the Director of National Intelligence could be held in contempt under Rule 6 as amended by the recently re-enacted information sharing amendments.

We hope you will find this information helpful. Please do not hesitate to contact the Department if we can be of assistance in other matters.

Sincerely,

A handwritten signature in black ink, reading "William E. Moschella". The signature is written in a cursive, slightly stylized font.

William E. Moschella  
Assistant Attorney General

Enclosure

cc: The Honorable Arlen Specter, Chairman  
Senate Committee on the Judiciary



U.S. Department of Justice  
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

April 30, 2002

The Honorable Patrick J. Leahy  
Chairman  
Committee on the Judiciary  
United States Senate  
Washington, D.C. 20510

Dear Mr. Chairman:

This letter provides the views of the Department of Justice and the Administration on S. 1615, the "Federal-Local Information Sharing Partnership Act of 2001." The Department of Justice supports the objectives of S. 1615 and supports six of its nine substantive provisions (sections 5 - 10) essentially as written. With respect to sections 2 - 4 of the bill, we recommend alternative language that we believe will better accomplish the bill's objectives.

As we understand it, S. 1615 is designed to provide federal law enforcement officials more consistent authority to share accurate, timely, and credible threat information with state and local officials, as appropriate for the performance of their duties. The close cooperation of federal, state, and local officials is critical to the ongoing effort against terrorism. We fully agree that there should be no unnecessary statutory constraints on the authority of federal officials to share information and coordinate with their state and local counterparts in meeting this threat to the nation. Hence, we strongly endorse the basic objectives of S. 1615. We note, however, that the discretionary authority that would be conferred by the legislation will be interpreted consistent with the President's constitutional authority to protect sensitive national security information. We believe that in the normal course of events timely and credible threat information may be provided to state and local officials without the need to share sensitive foreign intelligence and counterintelligence information, including information regarding intelligence sources and methods. When it becomes necessary to share such sensitive information, the Attorney General will share foreign intelligence and counterintelligence information in a manner consistent with the President's constitutional authorities and only based on strict need-to-know principles. To enable the discretionary sharing of sensitive information, we propose modifying sections 2, 3, and 4 of the legislation to provide a direct role for the Director of Central Intelligence for drafting implementing guidelines.

The following presents our views on specific provisions of S. 1615. As noted above, we support sections 5-10 of S. 1615 substantially as written. Those provisions address the sharing of consumer information (section 5), visa information (section 6), FISA information (sections 7 and

8), and educational information (sections 9 and 10). We discuss each of those provisions below. We then address sections 2 - 4 of the bill and the alternative language we propose for each of those sections. Attached to this letter is a "redlined" version of Fed. R. Crim. P. 6(e), as it would appear if amended as we suggest.

#### Section 5: Consumer Information.

Section 626 of the Fair Credit Reporting Act, added by section 358(g) of the USA Patriot Act, directs consumer reporting agencies to provide a consumer report and all other information in a consumer's file to a government agency authorized to conduct investigations or intelligence or counterintelligence activities or analysis related to international terrorism, on certification by the government agency that the information is necessary for the agency's conduct of the investigation, activity, or analysis. Section 5 of S. 1615 would add language to this provision authorizing the federal agency to disclose the information to state and local law enforcement personnel. Information could be shared with state and local personnel only to assist them in the performance of their official duties, and state and local recipients could use the information only consistent with guidelines issued by the Attorney General to protect confidentiality. We believe that this is an appropriate expansion of current law.

#### Section 6: Visa Information.

Under 8 U.S.C. § 1202(f), records of the State Department and diplomatic and consular offices pertaining to the issuance or refusal of visas or permits to enter the United States shall generally be considered confidential, and shall be used only for the formulation, amendment, administration, or enforcement of the immigration, nationality, and other laws of the United States. Section 1202(f) states two exceptions to this rule: (1) the Secretary of State has discretion to make such records available to a court where needed in a pending case; and (2) the Secretary of State has discretionary authority to provide visa lookout information and other related records to foreign governments under certain circumstances. The latter exception was added by section 413 of the USA Patriot Act. However, no comparable provision was adopted to permit the sharing of visa-related information with state and local law enforcement.

Section 6 of S. 1615 proposes an additional exception, authorizing the Secretary of State to provide information within the scope of 8 U.S.C. § 1202(f) to state and local law enforcement personnel. As with the bill's provision governing consumer information (section 5), the disclosure of visa-related information would remain a matter of discretion on the part of the responsible federal official – here, the Secretary of State – and use of the information by state

and local recipients would be constrained by guidelines issued by the Attorney General to protect confidentiality.<sup>1</sup>

#### Sections 7 and 8: FISA Information.

Under 50 U.S.C. §§ 1806(k) and 1825(k), which were added by section 504 of the USA Patriot Act, federal officers conducting electronic surveillance or physical searches under the Foreign Intelligence Surveillance Act (FISA) may "consult with Federal law enforcement officers to coordinate efforts to investigate or protect against" specified foreign threats to U.S. national security. These provisions also create a safe harbor for such coordination by providing that it "shall not" preclude the certification by the government of the required "significant" foreign intelligence purpose for electronic surveillance or a physical search, or the entry of an order by the Foreign Intelligence Surveillance Court authorizing electronic surveillance or a physical search.

Sections 7 and 8 of S. 1615 would amend FISA to permit consultation with state and local law enforcement officers as well as federal law enforcement officers to coordinate efforts to protect national security.<sup>2</sup> We believe that there may be instances in which such coordination is necessary and appropriate, and we therefore support the extension of the safe harbor to consultations with state law enforcement officials.

#### Sections 9 and 10: Educational Records.

20 U.S.C. § 1232g(j) and 20 U.S.C. § 9007(c), which were added by sections 507 and 508 of the USA Patriot Act, provide access pursuant to court order to certain educational records and information for the purpose of investigating or prosecuting terrorism. Under these provisions, the information must be relevant to the investigation or prosecution of an offense listed in 18 U.S.C. § 2332b(g)(5)(B) or an act of domestic or international terrorism as defined in 18 U.S.C. § 2331. The information can be retained, disseminated, and used for official purposes

---

<sup>1</sup> Section 6 of the bill authorizes the Secretary of State to provide information "if the Secretary of State determines that it is necessary and appropriate." To be consistent with the USA Patriot Act information-sharing provisions and the amendments in other sections of the bill, the following language should be substituted for the quoted language: "to assist the official receiving that information in the performance of the official duties of that official." See, e.g., USA Patriot Act § 203(d); S. 1615, § 5.

<sup>2</sup> In the public law citation for 50 U.S.C. § 1806 in section 7 of the bill, the correct reference would be "[s]ection 106(k)(1)" of the Foreign Intelligence Surveillance Act, rather than "[s]ection 160(k)(1)."

related to investigation or prosecution of these offenses, consistent with guidelines issued by the Attorney General to protect confidentiality. Sections 9 and 10 of the bill would amend these provisions to add explicit language stating that the authorized dissemination of the information would include dissemination to state and local law enforcement personnel.

The proposed amendments in sections 9 and 10 of the bill largely amount to clarifying provisions in relation to current law. The general standard under current 20 U.S.C. § 1232g(j) and 20 U.S.C. § 9007(c) is that the information to be shared must be relevant to the investigation or prosecution of an offense listed in 18 U.S.C. § 2332b(g)(5)(B) or an act of domestic or international terrorism as defined in 18 U.S.C. § 2331. Domestic and international terrorism, as defined in 18 U.S.C. § 2331, includes acts "that are a violation of the criminal laws of the United States or of any State." Hence, under the natural reading of these provisions, dissemination of the information to federal, state, and local law enforcement in terrorism cases for the investigation or prosecution of either federal or state crimes is already authorized. The amendments in sections 9 and 10 will eliminate any possible uncertainty on this point, and fully equate information sharing under these provisions with information-sharing under the other USA Patriot Act provisions that the bill amends.<sup>3</sup>

#### Section 2: Grand Jury Information.

We support the objective of section 2 of S. 1615, which is to facilitate the sharing of certain matters occurring before the grand jury with state and local officials. We believe, however, that section 2 is too narrow in some respects and too broad in others.

Section 2 is too narrow in two respects. While it permits disclosure of foreign intelligence, foreign counterintelligence, and foreign intelligence information, section 2 does not permit the sharing of information relating solely to a domestic threat. In addition, while section 2 permits disclosure to state and local law enforcement personnel and chief executives, it does not authorize disclosure to foreign government personnel or to state protective or disaster relief personnel. As the recent anthrax incidents illustrate, it will not always be clear whether threats to public safety result from international or domestic terrorism, and thus whether such threats qualify as foreign intelligence, foreign counterintelligence, or foreign intelligence information. The anthrax incidents also show that the required response to terrorist acts is not exclusively a

---

<sup>3</sup> Sections 9 and 10 each refer to state and local recipients parenthetically following the word "disseminate" in the provisions they amend. To be consistent with the other USA Patriot Act information sharing provisions and the amendments in other sections of the bill, the concluding language in the parentheses should read "to assist the official receiving that information in the performance of the official duties of that official", rather than "in the performance of the official duties of that law enforcement officer". See, e.g., USA Patriot Act § 203(d); S. 1615, § 5.

law enforcement matter, but may implicate the responsibilities of public health officials and other officials whose duties include protection of the public from criminal activities or their consequences. Other hypothetical situations illustrate the need for disclosure to foreign officials – for example, information relating to an anthrax attack on London or an attempt to crash an airplane into the Eiffel Tower.

As indicated previously, however, not all foreign intelligence information is appropriate for dissemination to state and local (or foreign) officials. For example, foreign intelligence information is defined by Rule 6 to include information that "relates to ... the conduct of the foreign affairs of the United States." Fed. R. Crim. P. 6(e)(3)(C)(iv)(II)(bb). While such information may well be appropriate for disclosure to federal immigration, intelligence, or national defense personnel, as authorized by Fed. R. Crim. P. 6(e)(3)(C)(i)(V), it is highly unlikely to be useful to state law enforcement officials because the states do not have authority to engage in foreign affairs. Given the tremendous importance of grand jury secrecy (see, e.g., *United States v. Sells Engineering, Inc.*, 463 U.S. 418 (1983)), we believe that the disclosure provisions of Rule 6 should be as broad, but no broader, than necessary.

We also believe that Rule 6(e) should be expanded to permit the disclosure of matters occurring before the grand jury to foreign government officials to the same extent as such matters may be disclosed to state and local officials, whether or not the matters involve threats of terrorism or related concerns. Under current law, an attorney for the federal government may unilaterally disclose such matters to state and local officials to assist in the enforcement of federal criminal law,<sup>4</sup> and may do so upon the approval of the court to assist in the enforcement of state criminal law.<sup>5</sup> With the increase in international travel and communications, there may be situations in which a federal prosecutor needs to disclose matters occurring before the grand jury to foreign officials as well as to state and local officials for conventional law enforcement purposes. Rule 6 should be amended to permit that disclosure.

In light of the foregoing concerns, we propose the following substitute for section 2:

(a) Rule 6(e)(3) of the Federal Rules of Criminal Procedure is amended –

(1) in subparagraph (A)(ii), by inserting "or of a foreign government" after "(including personnel of a state or subdivision of a state";

(2) in subparagraph (C)(i)(IV) –

---

<sup>4</sup> See Rule 6(e)(3)(A)(ii).

<sup>5</sup> See Rule 6(e)(3)(C)(i)(IV).

(A) by inserting "or foreign" after "may disclose a violation of State"; and

(B) by inserting "or of a foreign government" after "to an appropriate official of a State or subdivision of a State"; and

(3) in subparagraph (C) (i)(I), by inserting before the semicolon the following: "or, upon a request by an attorney for the government, when sought by a foreign court or prosecutor for use in an official criminal investigation".

(b) Rule 6(e) of the Federal Rules of Criminal Procedure is amended –

(1) in paragraph (3)(C)(i) –

(A) by striking "or" at the end of subclause (IV);

(B) by striking the period at the end of subclause (V) and inserting "; or"; and

(C) by adding at the end the following:

"(VI) when the matters involve a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, to any appropriate federal, state, local, or foreign government official for the purpose of preventing or responding to such a threat."; and

(2) in paragraph (3)(C)(iii) –

(A) by striking "Federal";

(B) by inserting "or clause (i)(VI)" after "clause (i)(V)"; and

(C) by adding at the end the following: "Any state, local, or foreign official who receives information pursuant to clause (i)(VI) shall only use that information consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue."; and

(3) in paragraph (2), by inserting "or of guidelines jointly issued by the Attorney General and Director of Central Intelligence pursuant to Rule 6" after "Rule 6".



Subsection (a)(1)-(2) of the Department's proposal amends Rule 6(e)(3)(A)(ii) and (C)(i)(IV) to permit disclosure of matters occurring before the grand jury to foreign government officials to the same extent as the Rule now permits such disclosure to state and local government officials. As noted above, we believe such amendments are appropriate in light of the increasing need for cooperation between U.S. and foreign officials in fighting terrorism and crime. These amendments are not limited to information concerning threats of attack, terrorism or the like; rather, they apply to information concerning all crimes, including more routine offenses (*e.g.*, information revealing an international scheme to defraud U.S. or foreign victims). These amendments do not establish any new or more expansive protocols for sharing information; they merely allow disclosure to foreign officials under the protocols that have governed disclosures to state and local officials since before the USA Patriot Act.

Subsection (a)(3) of the proposal makes a related change in Rule 6(e)(3)(C)(i)(I) to permit disclosure of matters occurring before the grand jury, as ordered by the court, where an attorney for the government requests the disclosure and a foreign court or prosecutor is seeking the information for use in an official criminal investigation. The desirability of this amendment was made clear following the September 11 terrorist attacks, when the international community rallied to cooperate in criminal investigations. It will clarify the power of the district judge, upon motion by the prosecutor, to authorize disclosure of grand jury information to a foreign judicial officer, prosecutor, or investigator who has formally requested it for use in a foreign criminal investigation. The amendment is needed in addition to the proposed changes to Rule 6(e)(3)(C)(i)(IV) and the proposed addition of Rule 6(e)(3)(C)(i)(VI) (discussed below).

Foreign prosecutors or investigating courts seeking evidence in the United States make requests under mutual legal assistance treaties or in letters rogatory pursuant to 28 U.S.C. § 1782. U.S. prosecutors actively assist the foreign authorities to obtain the evidence. On occasion, providing the evidence may require disclosure of grand jury information. However, even when the government makes an appropriate showing to the court (*i.e.*, a showing similar to that required for disclosure of grand jury material in a domestic proceeding), the rule as currently written does not expressly authorize courts to order disclosure. As a consequence, the U.S. prosecutor sometimes must re-subpoena the same information from the original sources. That process is cumbersome, it may unnecessarily inconvenience the persons or entities that already provided the information to the grand jury, and it is time-consuming. These difficulties and delays can affirmatively impede the foreign investigation. Moreover, certain evidence – such as witness testimony or original documents – simply cannot be obtained through alternative means. The foreign investigation may thus be thwarted, even though the evidence is available. If Rule 6 is clarified in accordance with this proposal, that evidence could be disclosed in appropriate circumstances.

Subsection (b) of the proposal deals with situations in which matters occurring before the grand jury reveal a threat of attack, sabotage, terrorism, or clandestine intelligence-gathering

activities. It adds a new subclause (VI) to Rule 6(e)(3)(C)(i) for this purpose. The description of matters that may be disclosed is derived from the definition of "foreign intelligence information" in Rule 6(e)(3)(C)(iv), which in turn is derived from 50 U.S.C. § 1801(e), the definition of "foreign intelligence information" in the Foreign Intelligence Surveillance Act. Our proposal is narrower than these provisions, however, because it omits what is referred to as "affirmative" foreign intelligence information, Rule 6(e)(3)(C)(iv)(II), 50 U.S.C. § 1801(e)(2), and adopts only the portion of the definition describing "protective" foreign intelligence, Rule 6(e)(3)(C)(iv)(I), 50 U.S.C. § 1801(e)(1). However, the proposal expands the definition of "protective" foreign intelligence to include not only international terrorism and sabotage committed by foreign powers and their agents, but also domestic terrorism and sabotage. Thus, for example, it would allow disclosure of information relating to the recent anthrax attacks regardless of whether they were committed by domestic terrorists (e.g., Timothy McVeigh) or international terrorists (e.g., Usama Bin Laden).<sup>6</sup>

In allowing disclosure of threat information to "appropriate" officials, subsection (b) of the Department's proposal follows the model of Rule 6(e)(3)(C)(i)(IV), which allows disclosure of matters occurring before the grand jury to "appropriate" state and local officials upon a court order. The proposal therefore differs from Rule 6(e)(3)(C)(i)(V), as added by section 203(a) of the USA Patriot Act, which allows disclosure of matters occurring before the grand jury to several designated categories of federal officials.<sup>7</sup>

Subsection (b) of the Department's proposal contains safeguards against the misuse of threat information. It follows Rule 6(e)(3)(C)(i)(IV) in permitting disclosure only for a specified

---

<sup>6</sup> Subsection (b) of the Department's proposal would not diminish existing authority, added by section 203(a) of the USA Patriot Act, to disclose foreign intelligence, foreign counterintelligence, and foreign intelligence information to designated federal officials. Rule 6(e)(3)(C)(i)(V). As noted above, such information is not limited to threat information, and we believe the broader grant of authority is appropriate with respect to federal officials whose responsibilities can include foreign affairs. Nor would subsection (b) conflict with authority to disclose information to state, local, or foreign officials for law enforcement purposes under Rules 6(e)(3)(A)(ii) and (C)(i)(IV) as amended by subsection (a) of the Department's proposal. To the extent that the duty to enforce criminal law does not include preventing or responding to threats to public safety, subsection (b) of our proposal makes clear that disclosure is nonetheless permitted, not only to law enforcement personnel, but also to other personnel whose duties do not include law enforcement (e.g., public health officials).

<sup>7</sup> Cf., current Rule 6(e)(3)(A)(ii) (permitting disclosure to "such [federal, state and local] government personnel" as are "deemed necessary by an attorney for the government" without a court order).

purpose – "preventing or responding to" a threat. It also amends Rule 6(e)(3)(C)(iii) to provide that recipients may use the disclosed information only as necessary in the conduct of their official duties and subject to limits on unauthorized disclosure and guidelines issued by the Attorney General. The use of Attorney General guidelines, which like much of our proposal is derived directly from S. 1615, protects information beyond what was required for disclosures under Rule 6(e)(3)(C)(i)(V) as added by the USA Patriot Act. Finally, subsection (b) of the proposal makes clear that knowing violations of the Attorney General's guidelines, like knowing violations of Rule 6 itself, are subject to punishment as a contempt of court under Rule 6(e)(2).

### Section 3: Wiretap Information.

We have similar concerns, and a similar proposal, with respect to section 3 of S. 1615, which deals with information obtained or derived from a domestic criminal wiretap pursuant to 18 U.S.C. §§ 2510, et seq. As added by section 203(b) of the USA Patriot Act, 18 U.S.C. § 2517(6), like its counterpart Fed. R. Crim. P. 6(e)(3)(C)(i)(V), permits disclosure of foreign intelligence, foreign counterintelligence, and foreign intelligence information to designated federal officials. Again, we believe that section 3 of the bill is too narrow in some respects and too broad in other respects, and we therefore propose the following alternative language:

Section 2517 of title 18, United States Code, is amended by adding at the end the following:

"(7) Any investigative or law enforcement officer, or attorney for the government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to a foreign investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure, and foreign investigative or law enforcement officers may use or disclose such contents or derivative evidence to the extent such use or disclosure is appropriate to the proper performance of their official duties.

"(8) Any investigative or law enforcement officer, or attorney for the government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to any appropriate federal, state, local, or foreign government official to the extent that such contents or derivative evidence reveals a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, for the purpose of preventing or responding to such a threat. Any official who receives information pursuant to this provision may use it only as

necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information, and any state, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue."

Following the model of 18 U.S.C. § 2517(3), this proposal refers to officers or attorneys who acquire knowledge of the "contents" of a communication or "evidence derived therefrom," and expressly authorizes disclosure of both "such contents" and of "such derivative evidence." Although 18 U.S.C. § 2517(1), (2) and (6) are phrased similarly, they expressly authorize disclosure of "such contents" but do not refer to disclosure of "such derivative evidence." We do not believe the omission indicates an intent to bar the disclosure of derivative evidence as opposed to the contents of communications themselves, but we would support conforming amendments to section 2517(1), (2) and (6) to avoid any ambiguity on the matter.

#### Section 4: Foreign Intelligence Information.

Section 4, like sections 2 and 3, expands existing authority to disseminate foreign intelligence and counterintelligence information to state and local officials, and therefore raises the same concerns as discussed above. To clarify these provisions, the Committee's report should highlight the central principles that continue to govern the dissemination of foreign intelligence and counterintelligence information: the President's constitutional authority to protect national security information, the statutory obligation of the Director of Central Intelligence to protect intelligence sources and methods, the adherence to "need-to-know" principles, and other legal restrictions on the dissemination of sensitive foreign intelligence or counterintelligence information.

Section 4 would amend section 203(d)(1) of the USA Patriot Act, which authorizes dissemination of such information "notwithstanding any other law." To avoid any conflict between section 203(d)(1) and the proposals set forth above, while taking into account the heightened concerns surrounding the dissemination of foreign intelligence and counterintelligence information, we propose amending section 203(d)(1) by striking the phrase "Notwithstanding any other provision of law," and enacting the following new provision:

"It shall be lawful for information revealing a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, obtained as part of a criminal investigation to be disclosed to any appropriate federal, state, local, or foreign government official for the purpose of preventing or responding to such a threat. Any official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject

to any limitations on the unauthorized disclosure of such information, and any state, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the Director of Central Intelligence and Attorney General shall jointly issue."

Because time may be of the essence in quickly disseminating information about emerging threats, the Administration will examine methods to ensure timely review of foreign intelligence and counterintelligence information when it is determined that such information should be disseminated to state and local officials.

To ensure consistency with the requirement of section 203(c) of the USA Patriot Act, which requires the Attorney General to establish procedures for the disclosure of information pursuant to Rule 6(e)(3)(C)(i)(V) and 18 U.S.C. §2517(6) that identifies a United States person, we propose the following provision:

Section 203(c) of Public Law 107-56 is amended by –

(1) inserting "and (8)" after "section 2517(6)"; and

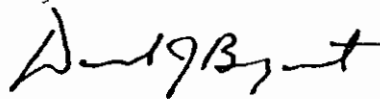
(2) inserting "and (VI)" after "Rule 6(e)(3)(C)(i)(V)".

We believe that the foregoing proposals would appropriately broaden federal information-sharing authority while preserving adequate safeguards against any potential misuse of the information. Following the general approach of the provisions which now appear in S. 1615, our alternative proposals for sections 2, 3, and 4 of the bill – relating to grand jury, wiretap, and "foreign intelligence" information – include requirements that state, local, and foreign recipients use shared information only in conformity with guidelines issued by the Attorney General and Director of Central Intelligence, and only as necessary in the conduct of their official duties subject to any limitations on unauthorized disclosure. Other limitations and safeguards which now apply in relation to federal officials who receive information would also be extended, as relevant, in relation to non-federal recipients. These include the requirement that the court be informed of the disclosure of grand jury information and the departments, agencies, or entities to which the disclosure is made (see Rule 6(e)(3)(C)(iii)), and the procedures established by the Attorney General (as required by section 203(c) of the USA Patriot Act) for the disclosure of wiretap and grand jury information that identifies a United States person. Moreover, it is important to emphasize that none of the provisions in S. 1615 and none of the proposals set forth in this letter *mandates* the disclosure or sharing of information; they only broaden discretionary authority to make disclosures. Hence, the Attorney General will retain the authority to adopt any additional standards and procedures he deems appropriate governing the disclosure of information within the scope of these provisions by Department of Justice personnel, whether to federal or non-federal recipients.

In sum, we support the enactment of S. 1615 as modified by the proposals set forth above, which we believe will achieve the legislation's objectives more effectively and completely.

Thank you for the opportunity to provide our views on this important matter. Please do not hesitate to call upon us if we may be of additional assistance. The Office of Management and Budget advises that there is no objection to the submission of this report from the standpoint of the Administration's program.

Sincerely,

A handwritten signature in black ink, appearing to read "D. J. Bryant", with a stylized flourish at the end.

Daniel J. Bryant  
Assistant Attorney General

cc: The Honorable Orrin G. Hatch  
Ranking Minority Member

Federal Rule of Criminal Procedure 6(e)  
as it would appear if amended as suggested in this letter  
(additions in redline text and deletions in ~~strikeout~~ text)

**Rule 6. The Grand Jury**

\* \* \* \*

**(e) Recording and Disclosure of Proceedings.**

(1) Recording of Proceedings. All proceedings, except when the grand jury is deliberating or voting, shall be recorded stenographically or by an electronic recording device. An unintentional failure of any recording to reproduce all or any portion of a proceeding shall not affect the validity of the prosecution. The recording or reporter's notes or any transcript prepared therefrom shall remain in the custody or control of the attorney for the government unless otherwise ordered by the court in a particular case.

(2) General Rule of Secrecy. A grand juror, an interpreter, a stenographer, an operator of a recording device, a typist who transcribes recorded testimony, an attorney for the government, or any person to whom disclosure is made under paragraph (3)(A)(ii) of this subdivision shall not disclose matters occurring before the grand jury, except as otherwise provided for in these rules. No obligation of secrecy may be imposed on any person except in accordance with this rule. A knowing violation of Rule 6 or of guidelines jointly issued by the Attorney General and Director of Central Intelligence pursuant to Rule 6 may be punished as a contempt of court.

**(3) Exceptions.**

(A) Disclosure otherwise prohibited by this rule of matters occurring before the grand jury, other than its deliberations and the vote of any grand juror, may be made to--

(i) an attorney for the government for use in the performance of such attorney's duty; and

(ii) such government personnel (including personnel of a state or subdivision of a state or of a foreign government) as are deemed necessary by an attorney for the government to assist an attorney for the government in the performance of such attorney's duty to enforce federal criminal law.

(B) Any person to whom matters are disclosed under subparagraph (A)(ii) of this paragraph shall not utilize that grand jury material for any purpose other than assisting the attorney for the government in the performance of such attorney's duty to enforce federal criminal law. An attorney for the government shall promptly provide the district court, before

which was impaneled the grand jury whose material has been so disclosed, with the names of the persons to whom such disclosure has been made, and shall certify that the attorney has advised such persons of their obligation of secrecy under this rule.

(C)(i) Disclosure otherwise prohibited by this rule of matters occurring before the grand jury may also be made –

(I) when so directed by a court preliminarily to or in connection with a judicial proceeding or, upon a request by an attorney for the government, when sought by a foreign court or prosecutor for use in an official criminal investigation;

(II) when permitted by a court at the request of the defendant, upon a showing that grounds may exist for a motion to dismiss the indictment because of matters occurring before the grand jury;

(III) when the disclosure is made by an attorney for the government to another Federal grand jury;

(IV) when permitted by a court at the request of an attorney for the government, upon a showing that such matters may disclose a violation of State or foreign criminal law, to an appropriate official of a State or subdivision of a State or of a foreign government for the purpose of enforcing such law;

(V) when the matters involve foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in clause (iv) of this subparagraph), to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties; or

(VI) when the matters involve a threat of actual or potential attack or other grave hostile acts when the matters involve a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, to any appropriate federal, state, local, or foreign government official for the purpose of preventing or responding to such a threat.

(ii) If the court orders disclosure of matters occurring before the grand jury, the disclosure shall be made in such manner, at such time, and under such conditions as the court may direct.



(iii) Any Federal official to whom information is disclosed pursuant to clause (i)(V) or clause (i)(VI) of this subparagraph may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information. Within a reasonable time after such disclosure, an attorney for the government shall file under seal a notice with the court stating the fact that such information was disclosed and the departments, agencies, or entities to which the disclosure was made. Any state, local, or foreign official who receives information pursuant to clause (i)(VI) shall only use that information consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue.

(iv) In clause (i)(V) of this subparagraph, the term "foreign intelligence information" means –

(I) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against –

(aa) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(bb) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(cc) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of foreign power; or

(II) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to –

(aa) the national defense or the security of the United States; or

(bb) the conduct of the foreign affairs of the United States.

(D) A petition for disclosure pursuant to subdivision (e)(3)(C)(i)(I) shall be filed in the district where the grand jury convened. Unless the hearing is ex parte, which it may be when the petitioner is the government, the petitioner shall serve written notice of the petition upon (i) the attorney for the government, (ii) the parties to the judicial proceeding if disclosure is sought in connection with such a proceeding, and (iii) such other persons as the court may direct. The court shall afford those persons a reasonable opportunity to appear and be heard.

(E) If the judicial proceeding giving rise to the petition is in a federal district court in another district, the court shall transfer the matter to that court unless it can reasonably obtain sufficient knowledge of the proceeding to determine whether disclosure is proper. The court shall order transmitted to the court to which the matter is transferred the material sought to be disclosed, if feasible, and a written evaluation of the need for continued grand jury secrecy. The court to which the matter is transferred shall afford the aforementioned persons a reasonable opportunity to appear and be heard.

(4) Sealed Indictments. The federal magistrate judge to whom an indictment is returned may direct that the indictment be kept secret until the defendant is in custody or has been released pending trial. Thereupon the clerk shall seal the indictment and no person shall disclose the return of the indictment except when necessary for the issuance and execution of a warrant or summons.

(5) Closed Hearing. Subject to any right to an open hearing in contempt proceedings, the court shall order a hearing on matters affecting a grand jury proceeding to be closed to the extent necessary to prevent disclosure of matters occurring before a grand jury.

(6) Sealed Records. Records, orders and subpoenas relating to grand jury proceedings shall be kept under seal to the extent and for such time as is necessary to prevent disclosure of matters occurring before a grand jury.



U. S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

November 12, 2003

The Honorable Thomas M. Davis III  
Chairman  
Committee on Government Reform  
U.S. House of Representatives  
Washington, DC 20515

Dear Mr. Chairman:

This provides the views of the Department of Justice on one provision of S. 589, the "Homeland Security Federal Workforce Act," as passed by the Senate. Title I of S. 589 establishes a pilot program for student loan repayment for Federal employees in areas of critical importance to the national security. We support measures to recruit and retain capable individuals for service in the Federal Government. There is serious doubt, however, about the constitutionality of the following provision contained in S. 589 (proposed 5 U.S.C. § 5379a(g)) --

(g) In selecting employees to receive benefits under this section, an agency shall, consistent with the merit system principles set forth in paragraphs (1) and (2) of section 2301(b) of this title, take into consideration the need to maintain a balanced workforce in which women and members of racial and ethnic minority groups are appropriately represented in Government service.

There is a significant risk that a court would determine that this provision encourages the consideration of race and ethnicity as factors in government decision-making, rendering it a classification that must pass strict judicial scrutiny (*i.e.*, it must be narrowly tailored to serve a compelling governmental interest).<sup>1</sup> See Lutheran Church

<sup>1</sup> It is also difficult to see how this provision could be reconciled with section 2301(b)(2) of title 5, United States Code, which provides that

"All employees and applicants for employment should receive fair and equitable treatment in all aspects of personnel management without regard

Missouri-Synod v. FCC, 141 F.3d 344, 352 (D.C. Cir. 1998) ("Lutheran Church I") (FCC regulations that "pressure stations to maintain a workforce that mirrors the racial breakdown of their metropolitan statistical area" deemed a racial classification); Lutheran Church Missouri-Synod v. FCC, 154 F.3d 487, 492 (D.C. Cir. 1998) ("Lutheran Church II") ("the regulations here must be subjected to strict scrutiny because they encourage racial preferences in hiring and as such treat people differently according to race"); *id.* at 491 ("Because the FCC's regulations at issue here indisputably pressure – even if they do not explicitly direct or require – stations to make race-based hiring decisions . . . they too must be subjected to strict scrutiny"); Schurr v. Resorts Int'l Hotel, Inc., 196 F.3d 486, 494 (3d Cir. 1999) (strict scrutiny applies where a regulation has "the practical effect of encouraging . . . discriminatory hiring"); Monterey Mechanical Co. v. Wilson, 125 F.3d 702, 710 (1997) (strict scrutiny applies where a statute "authorizes or encourages" a racial preference) (quoting Bras v. California Pub. Utilities Comm'n, 59 F.3d 869, 875 (9th Cir. 1995)).<sup>2</sup> This provision of S. 589 is unlikely to survive this analysis.

The Supreme Court has only recognized two compelling interests in recent years justifying the consideration of race or ethnicity by a government agency. First, the government has a compelling interest in acting to remedy the identified effects of its own discrimination. See City of Richmond v. J.A. Croson Co., 488 U.S. 469, 486 (1989); Wygant v. Jackson Bd. of Educ., 476 U.S. 267, 274 (1986). Second, the government has a compelling interest in obtaining the educational benefits that flow from a diverse student body. Grutter v. Bollinger, 2003 WL 21433492 \* – (June 23, 2003) ("student body diversity is a compelling state interest that can justify the use of race in university admissions."). It does not appear that this provision of S. 589 is designed to address the former interest, and the provision clearly does not rely on the latter. In the absence of a compelling governmental interest, consideration of race is constitutionally impermissible.

Even assuming the existence of a compelling governmental interest, the provision would likely fail narrow tailoring analysis, because it seeks to maintain, rather than attain,

---

to political affiliation, *race, color*, religion *national origin*, *sex*, marital status, age, or handicapping condition, and with proper regard for their privacy and constitutional rights."

(Emphasis added.)

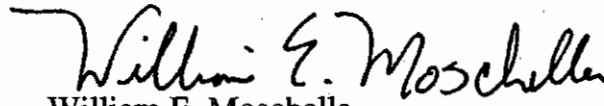
<sup>2</sup> Although classifications based on race receive strict scrutiny, classifications based on gender receive "intermediate scrutiny" (i.e., such classifications must serve "important governmental objectives," and the means must be "substantially related to the achievement of those goals"). United States v. Virginia, 518 U.S. 515, 533 (1996); Mississippi University for Women v. Hogan, 458 U.S. 718 (1982).

a diverse workforce. See Sheet Metal Workers' Int'l Ass'n v. EEOC, 478 U.S. 421, 477-78 (1986) (non-remedial racial preferences (preferences for a purpose other than remedying past discrimination) "may not be[] used simply to achieve and maintain racial balance"); Johnson v. Transportation Agency, Santa Clara County, 480 U.S. 616, 639 (1987) (approving affirmative action plan under Title VII that " was intended to attain a balanced workforce, not to maintain one").

In sum, it appears that this provision of S. 589 creates a racial classification yet fails both prongs of strict scrutiny analysis (i.e., it is not impelled by governmental interest and it is not narrowly tailored). Consequently, it is likely that this provision violates the equal protection component of the due process clause of the Fifth Amendment.

Thank you for your attention to this matter. Please feel free to call upon us if we may be of additional assistance. The Office of Management and Budget has advised that there is no objection from the standpoint of the Administration's program to the presentation of this report.

Sincerely,

  
William E. Moschella  
Assistant Attorney General

cc: The Honorable Henry A. Waxman  
Ranking Minority Member



U.S. Department of Justice

Office of Legislative Affairs

---

Washington, D.C. 20530

September 30, 2003

The Honorable Peter G. Fitzgerald  
Chairman  
Subcommittee on Financial Management, the Budget,  
and International Security  
Committee on Governmental Affairs  
United States Senate  
Washington, D.C. 20510

Dear Mr. Chairman:

This letter presents the views of the Department of Justice on S. 1229, the "Federal Employee Protection of Disclosures Act." We very strongly oppose this legislation.

S. 1229 would make a number of significant and extremely undesirable changes to the Whistleblower Protection Act ("WPA") and the Civil Service Reform Act ("CSRA"). Among other things, the bill would permit, for the first time, the Merit Systems Protection Board ("MSPB") and the courts to review the Executive branch's decisions regarding security clearances. It would provide new protections for the unauthorized disclosure of classified information. It would make sweeping changes to the WPA, including a vast expansion of the definition of a "protected disclosure." It would alter the carefully crafted scheme for judicial review of decisions of the MSPB, which is set forth in the CSRA. It would grant the Office of Special Counsel independent litigating authority. S. 1229 is burdensome, unnecessary, and unconstitutional. Rather than promote and protect genuine disclosures of matters of real public concern, it would provide a legal shield for unsatisfactory employees. *See, e.g.,* S. Rep. No. 100-413, at 15 (1988) ("The Committee does not intend that employees who are poor performers escape sanction by manufacturing a claim of whistleblowing"); S. Rep. No. 95-969, at 8, *reprinted in* 1978 U.S.S.C.A.N. 2723, 2730-31 ("Nor would the bill protect employees who claim to be whistle blowers in order to avoid adverse action based on inadequate performance").

### **Constitutional Concerns**

Section 1(b) of the bill would create 5 U.S.C. § 2302(b)(8)(C). This new section would protect the unauthorized disclosure of classified information to certain members of Congress and to Executive branch or to congressional employees with appropriate clearance. Under the new section, any Federal employee with access to classified information that – in the employee's sole opinion – indicated misconduct could share that information with certain members of Congress or of the Executive branch. The disclosure of that information could be made regardless of any restrictions or Executive branch authorization procedures established by the President and the

employee could not be disciplined for such an unauthorized disclosure. We believe that this new provision would be unconstitutional.

This new section would authorize any Federal employee to determine unilaterally how, when, and under what circumstances classified information will be shared with others, regardless of Presidential determinations that access be limited. Thus, it would interfere with the President's constitutional authority to protect national security information and therefore would violate the constitutional separation of powers. The constitutional authority of the President to take actions as Chief Executive and Commander-in-Chief of the armed forces of the United States grants the Executive branch the authority to

classify and control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to occupy a position . . . that will give that person access to such information . . . [This authority] flows primarily from this constitutional investment of power and exists quite apart from any explicit congressional grant.

*Department of the Navy v. Egan*, 484 U.S. 518, 524 (1988); *see also United States v. Nixon*, 418 U.S. 683, 706, 710, 712 n.19 (1974) (emphasizing heightened status of the President's constitutional privilege in the context of military, diplomatic, or sensitive national security secrets); *New York Times Co. v. United States*, 403 U.S. 713, 729-30 (1971) (Stewart, J., concurring) ("it is the constitutional duty of the Executive . . . to protect the confidentiality necessary to carry out its responsibilities in the fields of international relations and national defense"); *United States v. Reynolds*, 345 U.S. 1, 7-8 (1953) (recognizing privilege in judicial proceedings for "state secrets" based on determination by senior Executive officials); *Guillot v. Garrett*, 970 F.2d 1320, 1324 (4th Cir. 1992) (President has "exclusive constitutional authority over access to national security information"); *Dorfmont v. Brown*, 913 F.2d 1399, 1404 (9th Cir. 1990), *cert. denied*, 499 U.S. 905 (1991) (Kozinski, J., concurring) (Constitution vests President with unreviewable discretion over security decisions made pursuant to his powers as chief executive and Commander-in-Chief).

Although the new section would limit the protected disclosures to congressional oversight committees or individuals with appropriate clearances in Congress or the Executive branch, it nonetheless constitutes an unconstitutional interference with the President's constitutional responsibilities respecting national security and foreign affairs. Although the designated individuals might have appropriate clearances to receive the classified information, it is the President's prerogative to determine who has the need to know this information. Moreover, the President will have to base this determination upon particular – and perhaps currently unforeseeable – circumstances, dictating that the security or foreign affairs interests of the Nation dictate a particular treatment of classified information. A compromise of the President's authority in this area is an impermissible encroachment upon the President's ability to carry out one of his core executive functions.

Although we understand the important public interest in protecting whistleblowers, the decision whether and under what circumstances to disclose classified information must be made by someone who is acting pursuant to the official authority of the President and who ultimately is responsible to the President. The Constitution does not permit Congress to authorize subordinate Executive branch employees to bypass these orderly procedures for review and clearance by vesting them with a right to disclose classified information, without fear of discipline for the unauthorized disclosure.

We note that the prior Administration took this same position in 1998, strongly opposing, as unconstitutional, legislation that would have vested employees of the intelligence community with a unilateral right to disclose classified information to Congress. *See Disclosure of Classified Information to Congress: Hearing Before the Senate Select Committee on Intelligence*, 105th Cong. 41-61 (1998) (Statement of Randolph D. Moss, Deputy Assistant Attorney General).

### Other Concerns

#### 1. Expanded Definition Of Protected Disclosure

Subsection 1(b)(1)(A) of the bill would broaden the definition of “protected disclosure” by amending 5 U.S.C. § 2302(b)(8)(A) to state:

any disclosure of information by an employee or applicant, *without restriction to time, place, form, motive, context, or prior disclosure made to any person by an employee or applicant, including a disclosure made in the ordinary course of an employee’s duties* that the employee or applicant reasonably believes evidences

(i) *any violation of any law, rule, or, regulation, or*

(ii) *gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.* [emphasis added]

This amendment appears intended to override or supersede a series of decisions by the United States Court of Appeals for the Federal Circuit that defined the scope of disclosures covered by section 2302(b)(8). *See, e.g., Horton v. Dep’t of Navy*, 66 F.3d 279, 282 (Fed. Cir. 1995) (*Horton*) (complaints to wrongdoers are not protected whistleblowing); *Willis v. Dep’t of Agriculture*, 141 F.3d 1139, 1143-44 (Fed. Cir. 1998) (ordinary work disagreements not protected disclosures, nor are disclosures made during the course of performing ordinary job duties); *Meuwissen v. Dep’t of the Interior*, 234 F.3d 9, 12-14 (Fed. Cir. 2000) (discussion of matters already known does not constitute a covered disclosure); *LaChance v. White*, 174 F.3d 1378, 1381 (Fed. Cir. 1999) (*White*) (in determining whether a disclosure is covered, the Board should consider the motives of the employee making the disclosure). The Federal Circuit



precedent was useful to Federal agencies because it insulated them from having to defend against potentially burdensome whistleblower litigation involving no more than workplace disagreements, complaints by disgruntled employees, or matters that never were, in any real sense, “disclosed” to any individuals or organizations having any authority to address the disclosures.

The expanded definition in subsection 1(b)(1)(A) would upset the delicate balance between whistleblower protection and the ability of Federal managers to manage the workforce. The WPA already provides adequate protection for legitimate whistleblowers. The proposed expansive definition has the potential to convert any disagreement or contrary interpretation of a law, no matter how trivial or frivolous, into a whistleblower disclosure. It will not provide further protection to those with legitimate claims, who are covered by the existing law. It simply will increase the number of frivolous claims of whistleblower reprisal. Such an increase in the number of frivolous claims would impose an unwarranted burden upon Federal managers and, ultimately, the MSPB and the Federal Judiciary.

The Federal Circuit appropriately has recognized that the purposes of the WPA must be taken into account in determining whether a disclosure is one protected by the WPA. *Willis v. Department of Agriculture*, 141 F.3d 1139, 1143 (Fed. Cir. 1998) (observing that “[t]he purpose of the WPA is to encourage government personnel to disclose government wrongdoing to persons who may be in a position to remedy the problem without fearing retaliatory action by their supervisors or those who might be harmed by the disclosures.”). Accordingly, the court in *Willis* recognized that expressing disagreement with a supervisor's decision to that supervisor was not the type of disclosure protected by the WPA because it was not reporting the supervisor's wrongdoing to anyone in a position to take action. *Id.* Moreover, the court found that the WPA was not intended to protect reports of violations of laws, rules, or regulations that an employee made as a part of his everyday job responsibilities. *Id.* at 1143-44.

These limitations are reasonable and serve to further the purpose of the WPA to protect legitimate whistleblowers. By prohibiting the consideration of “time, place, form, motive, context” and including the performance of one’s job duties in the definition of “disclosures,” the bill converts every Federal employee into a whistleblower. Nearly every Federal employee will, sometime during the course of his or her career, disagree with a statement or interpretation made by a supervisor, or during the course of performing his or her everyday responsibilities, report an error that may demonstrate a violation of a law, rule, or regulation. Without the ability to take the context – the time, the place, the motive – of the alleged disclosure into account, even trivial or *de minimis* matters would become elevated to the status of protected disclosures. *Cf. Herman v. Department of Justice*, 193 F.3d 1375, 1378-79 (Fed. Cir. 1999) (concluding that the WPA was not intended to apply to trivial matters). This provision would undermine the effectiveness of the WPA.

The danger of this expanded definition is even more apparent when understood in the context of the statutory scheme of the WPA. Under current law, once an individual has made a

qualifying disclosure pursuant to 5 U.S.C. § 2302(b)(8), a *prima facie* case of whistleblower reprisal can be made by showing that a deciding agency official: a) knew of the disclosure; and b) an adverse action was taken within a reasonable time of the disclosure. *Kewley v. Department of Health & Human Serv.*, 153 F.3d 1357, 1362-62 (Fed. Cir. 1998) (citing 5 U.S.C. § 1221(e)(1)). Once the employee establishes this *prima facie* case, the burden shifts to the employing agency to show by clear and convincing evidence that it would have taken the adverse action regardless of the protected disclosure. *Kewley*, 153 F.3d at 1363.

Given the expanded definition of disclosure and the relatively light burden of establishing a *prima facie* case of reprisal under the knowledge/timing test, it would be exceedingly easy for employees to use whistleblowing as a defense to every adverse personnel action. Then the statutory structure of the WPA would require the agency to meet the much higher burden of demonstrating by clear and convincing evidence that it would have taken the adverse action, regardless of the disclosure. Thus, for all practical purposes, section 1(b)(1)(A) would transform the statutory standard that an agency must meet in sustaining almost every adverse action from a preponderance of the evidence, 5 U.S.C. § 7701(c)(1)(B), to the clear and convincing standard required by 5 U.S.C. § 1221(e)(2).

The ease with which a Federal employee would be able to establish a *prima facie* case of whistleblower reprisal, no matter how frivolous, would seriously impair the ability of Federal managers to effectively and efficiently manage the workforce. If Federal managers knew that it was likely that they would be subject to a charge of whistleblower reprisal every time that they took an adverse personnel action, they might hesitate to take any such action. Likewise, the very low standards that would be required to advance a whistleblower claim would vastly increase the number of such claims, obscure the claims of legitimate whistleblowers, and unduly burden the MSPB and the Federal Circuit.

Currently, the WPA does not cover disclosures that specifically are prohibited by law or disclosures of information that specifically are required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs. Subsection 1(b)(1)(B) would add 5 U.S.C. § 2302(b)(8)(C) to include this category of covered disclosures if the disclosure evidenced a reasonable belief of violation of law, rule, or regulation; gross mismanagement; gross waste of funds; abuse of authority; substantial and specific danger to public health or safety; or a false statement to Congress on an issue of material fact. The disclosure also would have to be made to a Member of Congress authorized to receive information of the type disclosed or to any employee of Congress having an appropriate security clearance and authorized to receive information of the type disclosed. The amendment would expand the scope of covered disclosures significantly and therefore substantially increase the potential exposure to litigation for Federal agencies as well as the staffing costs and other burdens associated with this issue.

Subsection 1(c) would amend 5 U.S.C. § 2302(b), adding at the end of that subsection a provision clarifying that a disclosure can be a formal or informal communication or transmission. As discussed above, this change appears intended to overrule or supersede contrary precedent by

the Federal Circuit limiting the scope of covered disclosures. *See Horton*, 66 F.3d at 282 (oral disclosures held not to be protected whistleblowing). This change would expand the class of covered disclosures and increase the scope of potential litigation on the issue of whistleblower reprisal. As a result, passing remarks made in the workplace or stray lines in electronic-mail messages on other subjects could potentially become the subject of whistleblower reprisal complaints.

## 2. Presumption of Good Faith

Subsection 1(d) would add at the end of 5 U.S.C. § 2302(b) a statement that “for the purposes of paragraph (8) any presumptions relating to the performance of a duty by an employee who has authority to take, direct others to take, recommend, or approve any personnel action may be rebutted by *substantial evidence*.” (emphasis added) This provision appears intended to supersede a holding in *White*, 174 F.3d at 1381, to the effect that analysis of the reasonableness of an employee’s belief in a disclosure should begin with the “presumption that public officials perform their duties correctly, fairly, in good faith and in accordance with the law and governing regulations.” *See id.* The court also held that this presumption can only be rebutted by “irrefragable proof to the contrary.” *See id.* The court has defined that standard of proof to be by clear and convincing evidence. *See Am-Pro Protective Agency, Inc. v. U.S.*, 281 F.3d 1234, 1239-40 (Fed. Cir. 2002). Subsection 1(d) would reverse a standard that was very helpful to Federal agencies in defending against whistleblower reprisal claims by challenging the reasonableness of employees’ beliefs in the validity of their disclosures. This provision would subject arguable or potentially questionable day-to-day management decisions to full-fledged litigation.

## 3. Security Clearances

There are three significant provisions regarding security clearances. First, subsection 1(e)(1) of the bill would amend 5 U.S.C. § 2302(a)(2)(A) to add “a suspension, revocation, or other determination relating to a security clearance,” to the definition of a personnel practice. Second, section 1(e)(2) (adding a new subparagraph (14) to 5 U.S.C. § 2302(b)) would amend the definition of prohibited personnel practices to include “conduct[ing] or caus[ing] to be conducted, an investigation of an employee or applicant for employment because of any activity protected under this section.” Third, subsection 1(e)(3) of the bill would authorize the MSPB and the courts to review these security clearance decisions to determine whether a violation of 5 U.S.C. § 2302 (prohibited personnel practices) had occurred and, if so, to order certain relief. We have both general and technical objections to these provisions.

We strongly oppose these amendments because they would authorize the MSPB and the courts to review any determination relating to a security clearance – a prerogative left firmly within the Executive branch's discretion. In *Egan*, 484 U.S. 518 (1988), the Supreme Court explicitly rejected the proposition that the MSPB and the Federal Circuit could review the decision to revoke a security clearance. In doing so, the Court relied upon a number of premises,

including: 1) decisions regarding security clearances are an inherently discretionary decision best left to the particular agency involved, not to be reviewed by non-expert bodies such as the MSPB and the courts; 2) review under the CSRA, which provides for a preponderance of the evidence standard, conflicts with the requirement that a security clearance should be given only when clearly consistent with the interests of the national security; and 3) that the President's power to make security clearance determinations is based in his constitutional role as Commander-in-Chief. See our constitutional objections at page 1, *supra*.

An example demonstrates one of the many fundamental problems with this bill's security clearance provisions. As we noted above, the burden of proof in CSRA cases is fundamentally incompatible with the standard for granting security clearances. This conflict is even more apparent in whistleblower cases. Under the WPA, a putative whistleblower establishes a *prima facie* case of whistleblower retaliation by establishing a protected disclosure and, under the knowledge/timing test, a personnel action taken within a certain period of time following the disclosure. Once the employee meets that minimal burden, the burden shifts to the agency to establish *by clear and convincing evidence* that it would have taken the action absent the protected disclosure.

Therefore, the bill would require in the security clearance context, that where individuals make protected disclosures (which, as we explain above, would include virtually every Federal employee under other amendments in this bill), the agency must justify its security clearance decision by the stringent standard of clear and convincing evidence. Thus, rather than awarding security clearances only where clearly consistent with the interests of national security, agencies would be permitted to deny or revoke them only upon the basis of clear and convincing evidence. This standard would be shockingly inconsistent with national security, especially in these times of heightened security concerns.

Beyond these objections, the amendments are simply unnecessary. Currently, Executive Order 12968 requires all agencies to establish an internal review board to consider appeals of security clearance revocations. These internal boards provide sufficient protections for the subjects of the revocations, while, at the same time, preserving the authority of the Executive branch to make the necessary decisions. In any event, we are not aware of any pattern of abusing security clearance decisions to retaliate against whistleblowers. Thus, the drastic and potentially unconstitutional amendments subsections 1(e)(1) and 1(e)(3) would make are unwarranted.

We have other, more specific, objections to the bill. In defining the category of security clearance decisions that fall within a personnel action and, therefore, would be subject to review, subsection 1(e)(1) of the bill uses the phrase "suspension, revocation, or *other determination* relating to a security clearance" [emphasis added]. The phrase "other determination" is vague and conceivably could encompass such things as an initial investigation into whether a security clearance is warranted, the decision to upgrade or downgrade a clearance, or any other decision connected in any way with a security clearance. This broad language would convert nearly every

action an agency takes with regard to a security clearance into a possible basis for a whistleblower charge.

In addition, section 1(e)(2), amending the definition of prohibited personnel practices to include “conduct[ing] or caus[ing] to be conducted, an investigation of an employee or applicant for employment because of any activity protected under this section,” is overly broad. As drafted, the provision could be construed to restrict the scope of routine employment inquiries to prior employers, where the Government was a prior employer. This might be the case, for example, where an employee left government service after a whistleblower situation and several years later applied for employment with a different Government agency, necessitating a new background investigation. Section 1(e)(2) would lead to disputes over the scope and permissibility of such inquiries. Moreover, the bar seems to apply whether the claim of whistleblower status was upheld or not.

Finally, section 1(e)(3) of the bill contains language stating that the MSPB or any reviewing court “may not order the President to restore a security clearance.” We presume this language was intended to alleviate concerns about the Executive branch prerogative with regard to security clearance determinations. However, the language, on its face, only prohibits the MSPB and reviewing court from ordering “the President” to “restore” a clearance. Conceivably, this language could be interpreted to allow the MSPB to order an agency head or lower official to restore the clearance. Likewise, it does not appear to limit the MSPB’s authority to order other actions with regard to security clearances, for instance, to award an initial clearance, to order an upgrade, or to stop an investigation. It also is unclear to us why a narrow class of whistleblower reprisal cases merits the “expedited review” section 1(3)(e) would require and what that would mean in this context.

#### 4. Confidential Advice on Making Disclosures to Congress

Subsection 1(j) would amend 5 U.S.C. § 2302(f) to require each agency to establish a procedure for providing confidential advice to employees on making lawful disclosures to Congress of information specifically required by law or Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs. This provision would place agencies in the odd and anomalous position of effectively encouraging their employees to disclose matters otherwise required by law to be kept secret. We oppose this provision.

#### 5. Compensatory Damages

Section 1(h) of the bill would allow the MSPB to award damages in corrective action cases, including compensatory damages. We oppose this provision. It would broaden whistleblower litigation to include disputes over allegations of mental and emotional stress, which are very vague, difficult to quantify, and correspondingly difficult to litigate. More importantly, it sets forth no limit upon the amount of compensatory damages that could be awarded and would have a chilling effect upon management decisions. Current law allows the

MSPB to award attorney's fees, back pay and related benefits, medical costs, travel expenses, and any other reasonable and foreseeable consequential damages. We believe that current law adequately compensates employees for whom corrective action is awarded.

## 6. Judicial Review

We object to section 1(k)(2) of the bill, which would grant the Office of Special Counsel the option to seek review of MSPB decisions by the regional courts of appeal rather than by the Federal Circuit. Review by the Federal Circuit promotes conformity in decisions and fosters uniformity in Federal personnel law. Granting the regional circuits jurisdiction to entertain appeals from the MSPB would undo Congress's sensible centralization of those appeals and further burden those already overburdened regional courts of appeal.

Since the enactment of the Federal Courts Improvement Act of 1982, the Federal Circuit has exercised exclusive jurisdiction to consider appeals from the MSPB in cases not involving discrimination. In those years, the court has developed substantial expertise and a well-defined body of law regarding Federal personnel matters that inures to the benefit of both the Federal Government and its employees. Moreover, the court's rules, which provide for more expedited and informal briefing in *pro se* cases provide an added benefit for Federal employees, many of whom choose to appeal the MSPB's decisions without the aid of an attorney.

Replacing the Federal Circuit's exclusive jurisdiction with review by the regional circuits would result in a fractured personnel system. Inevitably, conflicts among the circuits would arise as to the proper interpretation of the Federal personnel laws, so that an employee's rights and responsibilities would be determined by the geographic location of his or her place of employment. Not only is a non-uniform system undesirable, it could contribute to a loss of morale, as Federal employees would be treated differently depending upon where they lived. Inevitably, it would require the Supreme Court to intervene more often in Federal personnel matters to resolve inconsistencies among the circuits.

The CSRA and the Federal Courts Improvement Act resolved the problems of regional review. Considering the Federal Circuit's now substantial expertise, there simply is no good reason to revert to the old system. We have similar concerns about section 1(l) (amending 5 U.S.C. § 7703(b) and (d)).

## 7. Litigating Authority For The Special Counsel

Section 1(k) of the bill would expand the authority of the Special Counsel by authorizing her to seek review unilaterally in the United States Court of Appeals for the Federal Circuit in any case to which she was a party, *see* section 1(k)(2) (adding new 5 U.S.C. § 7703(e)(1)), and by granting her the authority to designate attorneys to appear upon her behalf in all courts except the Supreme Court, *see* section 1(k)(1) (adding new 5 U.S.C. § 1212(h)). Current law authorizes the Special Counsel to appear only before the MSPB. We oppose both of these changes.

Under current law, employees who are adversely affected by a decision of the MSPB have the right to appeal to the Court of Appeals for the Federal Circuit. *See* 5 U.S.C. § 7703(a). The Department of Justice represents the respondent Federal agencies in these appeals. Federal employing agencies do not possess the same right to appeal MSPB decisions adverse to them. OPM is the only Government agency that may appeal an MSPB decision and it may do so only after it has intervened in the MSPB proceeding to present its position and its director has determined that an MSPB decision rejecting OPM's position will have a "substantial impact" upon the administration of the civil service law. 5 U.S.C. § 7703(d). Moreover, once the director makes such a determination, OPM must seek authorization from the Justice Department's Solicitor General to file a petition for review. The Federal Circuit has discretion to grant or deny this petition. OPM is represented in the Federal Circuit by the Department of Justice.

Section 1(k)(2) of the bill would disrupt this carefully crafted scheme by authorizing the Special Counsel, without the approval of the Solicitor General, to petition the Federal Circuit for leave to appeal any adverse MSPB decision. The only limitation placed upon this right would be the requirement that the Special Counsel, if not a party to or intervenor in the matter before the MSPB, petition the MSPB for reconsideration of its decision before seeking review in the Federal Circuit.

Section 1(k)(1) would further erode centralized control over personnel litigation by authorizing the Office of the Special Counsel to represent itself in all litigation except litigation before the Supreme Court. This authority would be independent of the Department of Justice and could result in the Special Counsel litigating against other Executive branch agencies. This would usurp the Justice Department's traditional unifying role as the Executive branch's representative in court. We are unaware of any justification for eroding the Department's ability to fulfill its well-settled representative role.

Centralized control furthers a number of important policy goals, including the presentation of uniform positions on significant legal issues, the objective litigation of cases by attorneys unaffected by the parochial concerns of a single agency that might be inimical to the interests of the Government as a whole, and the facilitation of presidential supervision over Executive branch policies implicated in Government litigation. This policy benefits not only the Government but also the courts and citizens who, in the absence of the policy, might be subjected to uncoordinated and inconsistent positions on the part of the Government.

## 8. Investigations

Subparagraph 1(e)(1)(B) of the bill would amend 5 U.S.C. § 2302(a)(2)(A) to include within WPA-covered personnel actions "an investigation of an employee or applicant for employment because of any activity protected under this section." Additionally, subparagraph 1(e)(2)(C) would amend 5 U.S.C. § 2302(b) to forbid Federal employees to "conduct, or cause to



be conducted, an investigation of an employee or applicant for employment because of any activity protected under this section.”

We are very troubled by the breadth of these provisions and the effect they could have on the ability of agencies to function. The amendments do not define an “investigation.” Accordingly, it would appear that any type of inquiry by any agency, ranging from criminal investigation to routine background investigation for initial employment to investigation for determining eligibility for a security clearance to Inspector General investigation to management inquiries of potential wrongdoing in the workplace, all could be subject to challenge and litigation.

Conceivably, any time a supervisor suspected wrongdoing by an employee and determined to look into the matter, the “investigation” could be subject to challenge. Certainly, any time an Office of Inspector General, an Office of Professional Responsibility, or similar agency component began an investigation, the investigation immediately could become the subject of litigation. Through such litigation, employees would be able to delay or thwart any investigation into their own or others’ wrongdoing. This result could adversely affect the ability and perhaps even the willingness of supervisors to examine wrongdoing – which clearly is not a beneficial outcome for the efficient and effective operation of agencies. Indeed, this provision could allow an employee to litigate an action that has not been proposed. Thus, even before any discipline had been proposed or any charges brought, the employee could attempt to short circuit any inquiry into the situation. In this connection, we note that the Equal Employment Opportunity Commission has prohibited the filing of a formal complaint on a “proposal to take a personnel action, or other preliminary step to taking a personnel action.” *See* 29 C.F.R. § 1614.107(a)(5).

The CSRA is a careful balance between providing remedies for personnel actions that have been taken against Federal employees and permitting agencies to manage their workforces effectively. Subparagraphs 1(e)(1)(B) and 1(e)(2)(C) would upset that balance seriously, since an investigation is not an action against the employee but is a necessary government function for gathering facts about a wide range of matters so that informed decisions can be subsequently made.

Further, including conducting investigations and “causing them to be conducted” among the prohibited practices could decrease the willingness of any employee to report allegations of misconduct to an Office of Inspector General (“OIG”), which is generally responsible for conducting such investigations. Even the reporting of wrongdoing could be viewed as causing an investigation to be conducted and could subject not just investigators and managers but any employee who “causes” an investigation to be conducted to charges of committing a prohibited personnel practice.

Moreover, the allegation of a prohibited personnel practice in the form of an investigation could result in an investigation by the Office of Special Counsel into an open criminal or



administrative investigation and into open investigatory files, and then, pursuant to the OSC's statutory obligations, the reporting of that investigatory information to the complainant. Except in limited circumstances, open investigative files are not shared with other agencies or persons for several reasons, including the privacy interests of the subject and witnesses, and the protection of investigative techniques. Additionally, the Inspector General Act of 1978, as amended, 5 U.S.C. app. § 7(a), requires that the confidentiality of a Federal employee complainant be maintained "unless disclosure is unavoidable during the course of an investigation." Our concerns are amplified because of OSC's reporting of the progress of its investigation and its findings to the complainant. This reporting could compromise and undermine a legitimate law enforcement investigation.

#### 9. Attorneys Fees

Section 1(g) of the bill would amend 5 U.S.C. § 1204(m)(1) to provide that, in disciplinary action cases, a prevailing employee could obtain attorney fees from the agency at which the prevailing party was employed rather than, as currently exists, from the agency proposing the disciplinary action against the employee. Essentially, this provision would shift the burden for attorney fees from the Office of Special Counsel, the agency responsible for pursuing disciplinary actions, to the prevailing party's employing agency. We object to this change for at least two reasons. First, one of the general policies underlying fee-shifting provisions against the Government is ensuring that the Government acts responsibly. By shifting the burden from the agency responsible for taking disciplinary actions – the Special Counsel – to the employing agency, this amendment would eliminate this important check on the Special Counsel in considering which actions to pursue because even if the Special Counsel took an unjustified action, it will not have to bear the attorney fees. Second, this amendment is patently unfair to the employing agencies, which might disagree with the action the Special Counsel was pursuing but nevertheless would be responsible for any fees. Indeed, it is not uncommon that an agency will refuse to take a disciplinary action that is proposed by the Special Counsel, agreeing with a particular employee that no wrongdoing had been committed. If the employee hired an attorney and successfully defended himself against the Special Counsel before the MSPB or the Federal Circuit, the employing agency – who disagreed with the Special Counsel's actions – would be required to pay the fees.

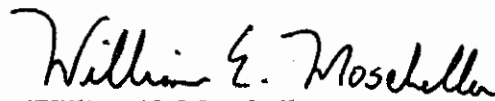
#### 10. Discipline Against Individual Agency Employees

Section 1(i) would amend 5 U.S.C. § 1215(a)(3) to allow for imposition of disciplinary action against an individual employee where the MSPB found that a prohibited personnel practice "was a motivating factor for the employee's decision to take . . . a personnel action, even if other factors also motivated the decision." Under this amendment, the board apparently could order discipline even if the agency proved by clear and convincing evidence that it would have taken the personnel action despite the protected disclosure. This amendment substantially lowers the burden for the Special Counsel to seek disciplinary actions and could result in managers being disciplined for retaliation even when the agency had met the high standard of showing that

the personnel action would have been taken in any event. Given the ease with which an employee could cloak himself in whistleblower status (based upon the bill's other provisions), this particular change would have a chilling effect on the ability of managers to take any negative personnel actions.

Thank you for the opportunity to present our views. Please do not hesitate to call upon us if we may be of additional assistance. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to submission of this report.

Sincerely,

A handwritten signature in black ink that reads "William E. Moschella". The signature is written in a cursive, flowing style.

William E. Moschella  
Assistant Attorney General

cc: The Honorable Daniel K. Akaka  
Ranking Minority Member



U.S. Department of Justice

Office of Legislative Affairs

Washington, D.C. 20530

November 10, 2003

The Honorable Peter G. Fitzgerald  
Chairman  
Subcommittee on Financial Management, the Budget,  
and International Security  
Committee on Governmental Affairs  
United States Senate  
Washington, D.C. 20510

Dear Mr. Chairman:

This letter presents the views of the Department of Justice on S. 1358, the "Federal Employee Protection of Disclosures Act." We very strongly oppose this legislation.

S. 1358 would make a number of significant and extremely undesirable changes to the Whistleblower Protection Act ("WPA") and the Civil Service Reform Act ("CSRA"). Among other things, the bill would permit, for the first time, the Merit Systems Protection Board ("MSPB") and the courts to review the Executive branch's decisions regarding security clearances. It would provide new protections for the unauthorized disclosure of classified information. It would make sweeping changes to the WPA, including a vast expansion of the definition of a "protected disclosure." It would alter the carefully crafted scheme for judicial review of decisions of the MSPB, which is set forth in the CSRA. It would grant the Office of Special Counsel independent litigating authority. S. 1358 is burdensome, unnecessary, and unconstitutional. Rather than promote and protect genuine disclosures of matters of real public concern, it would provide a legal shield for unsatisfactory employees. *See, e.g.,* S. Rep. No. 100-413, at 15 (1988) ("The Committee does not intend that employees who are poor performers escape sanction by manufacturing a claim of whistleblowing"); S. Rep. No. 95-969, at 8, *reprinted in* 1978 U.S.S.C.A.N. 2723, 2730-31 ("Nor would the bill protect employees who claim to be whistle blowers in order to avoid adverse action based on inadequate performance").

### Constitutional Concerns

Section 1(b) of the bill would create 5 U.S.C. § 2302(b)(8)(C). This new section would protect the unauthorized disclosure of classified information to certain members of Congress and to Executive branch or to congressional employees with appropriate clearance. Under the new section, any Federal employee with access to classified information that – in the employee's sole opinion – indicated misconduct could share that information with certain members of Congress or of the Executive branch. The disclosure of that information could be made regardless of any restrictions or Executive branch authorization procedures established by the President and the

employee could not be disciplined for such an unauthorized disclosure. We believe that this new provision would be unconstitutional.

This new section would authorize any Federal employee to determine unilaterally how, when, and under what circumstances classified information will be shared with others, regardless of Presidential determinations that access be limited. Thus, it would interfere with the President's constitutional authority to protect national security information and therefore would violate the constitutional separation of powers. The constitutional authority of the President to take actions as Chief Executive and Commander-in-Chief of the armed forces of the United States grants the Executive branch the authority to

classify and control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to occupy a position . . . that will give that person access to such information . . . [This authority] flows primarily from this constitutional investment of power and exists quite apart from any explicit congressional grant.

*Department of the Navy v. Egan*, 484 U.S. 518, 524 (1988); *see also United States v. Nixon*, 418 U.S. 683, 706, 710, 712 n.19 (1974) (emphasizing heightened status of the President's constitutional privilege in the context of military, diplomatic, or sensitive national security secrets); *New York Times Co. v. United States*, 403 U.S. 713, 729-30 (1971) (Stewart, J., concurring) ("it is the constitutional duty of the Executive . . . to protect the confidentiality necessary to carry out its responsibilities in the fields of international relations and national defense"); *United States v. Reynolds*, 345 U.S. 1, 7-8 (1953) (recognizing privilege in judicial proceedings for "state secrets" based on determination by senior Executive officials); *Guillot v. Garrett*, 970 F.2d 1320, 1324 (4th Cir. 1992) (President has "exclusive constitutional authority over access to national security information"); *Dorfmont v. Brown*, 913 F.2d 1399, 1404 (9th Cir. 1990), *cert. denied*, 499 U.S. 905 (1991) (Kozinski, J., concurring) (Constitution vests President with unreviewable discretion over security decisions made pursuant to his powers as chief executive and Commander-in-Chief).

Although the new section would limit the protected disclosures to congressional oversight committees or individuals with appropriate clearances in Congress or the Executive branch, it nonetheless constitutes an unconstitutional interference with the President's constitutional responsibilities respecting national security and foreign affairs. Although the designated individuals might have appropriate clearances to receive the classified information, it is the President's prerogative to determine who has the need to know this information. Moreover, the President will have to base this determination upon particular – and perhaps currently unforeseeable – circumstances, dictating that the security or foreign affairs interests of the Nation dictate a particular treatment of classified information. A compromise of the President's authority in this area is an impermissible encroachment upon the President's ability to carry out one of his core executive functions.

Although we understand the important public interest in protecting whistleblowers, the decision whether and under what circumstances to disclose classified information must be made by someone who is acting pursuant to the official authority of the President and who ultimately is responsible to the President. The Constitution does not permit Congress to authorize subordinate Executive branch employees to bypass these orderly procedures for review and clearance by vesting them with a right to disclose classified information, without fear of discipline for the unauthorized disclosure.

We note that the prior Administration took this same position in 1998, strongly opposing, as unconstitutional, legislation that would have vested employees of the intelligence community with a unilateral right to disclose classified information to Congress. *See Disclosure of Classified Information to Congress: Hearing Before the Senate Select Committee on Intelligence*, 105th Cong. 41-61 (1998) (Statement of Randolph D. Moss, Deputy Assistant Attorney General).

### Other Concerns

#### 1. Expanded Definition Of Protected Disclosure

Subsection 1(b)(1)(A) of the bill would broaden the definition of "protected disclosure" by amending 5 U.S.C. § 2302(b)(8)(A) to state:

any disclosure of information by an employee or applicant, *without restriction to time, place, form, motive, context, or prior disclosure made to any person by an employee or applicant, including a disclosure made in the ordinary course of an employee's duties* that the employee or applicant reasonably believes evidences

(i) *any violation of any law, rule, or regulation, or*

(ii) *gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.* [emphasis added]

This amendment appears intended to override or supersede a series of decisions by the United States Court of Appeals for the Federal Circuit that defined the scope of disclosures covered by section 2302(b)(8). *See, e.g., Horton v. Dep't of Navy*, 66 F.3d 279, 282 (Fed. Cir. 1995) (*Horton*) (complaints to wrongdoers are not protected whistleblowing); *Willis v. Dep't of Agriculture*, 141 F.3d 1139, 1143-44 (Fed. Cir. 1998) (ordinary work disagreements not protected disclosures, nor are disclosures made during the course of performing ordinary job duties); *Meuwissen v. Dep't of the Interior*, 234 F.3d 9, 12-14 (Fed. Cir. 2000) (discussion of matters already known does not constitute a covered disclosure); *LaChance v. White*, 174 F.3d 1378, 1381 (Fed. Cir. 1999) (*White*) (in determining whether a disclosure is covered, the Board should consider the motives of the employee making the disclosure). The Federal Circuit

precedent was useful to Federal agencies because it insulated them from having to defend against potentially burdensome whistleblower litigation involving no more than workplace disagreements, complaints by disgruntled employees, or matters that never were, in any real sense, "disclosed" to any individuals or organizations having any authority to address the disclosures.

The expanded definition in subsection 1(b)(1)(A) would upset the delicate balance between whistleblower protection and the ability of Federal managers to manage the workforce. The WPA already provides adequate protection for legitimate whistleblowers. The proposed expansive definition has the potential to convert any disagreement or contrary interpretation of a law, no matter how trivial or frivolous, into a whistleblower disclosure. It will not provide further protection to those with legitimate claims, who are covered by the existing law. It simply will increase the number of frivolous claims of whistleblower reprisal. Such an increase in the number of frivolous claims would impose an unwarranted burden upon Federal managers and, ultimately, the MSPB and the Federal Judiciary.

The Federal Circuit appropriately has recognized that the purposes of the WPA must be taken into account in determining whether a disclosure is one protected by the WPA. *Willis v. Department of Agriculture*, 141 F.3d 1139, 1143 (Fed. Cir. 1998) (observing that "[t]he purpose of the WPA is to encourage government personnel to disclose government wrongdoing to persons who may be in a position to remedy the problem without fearing retaliatory action by their supervisors or those who might be harmed by the disclosures."). Accordingly, the court in *Willis* recognized that expressing disagreement with a supervisor's decision to that supervisor was not the type of disclosure protected by the WPA because it was not reporting the supervisor's wrongdoing to anyone in a position to take action. *Id.* Moreover, the court found that the WPA was not intended to protect reports of violations of laws, rules, or regulations that an employee made as a part of his everyday job responsibilities. *Id.* at 1143-44.

These limitations are reasonable and serve to further the purpose of the WPA to protect legitimate whistleblowers. By prohibiting the consideration of "time, place, form, motive, context" and including the performance of one's job duties in the definition of "disclosures," the bill converts every Federal employee into a whistleblower. Nearly every Federal employee will, sometime during the course of his or her career, disagree with a statement or interpretation made by a supervisor, or during the course of performing his or her everyday responsibilities, report an error that may demonstrate a violation of a law, rule, or regulation. Without the ability to take the context – the time, the place, the motive – of the alleged disclosure into account, even trivial or *de minimis* matters would become elevated to the status of protected disclosures. *Cf. Herman v. Department of Justice*, 193 F.3d 1375, 1378-79 (Fed. Cir. 1999) (concluding that the WPA was not intended to apply to trivial matters). This provision would undermine the effectiveness of the WPA.

The danger of this expanded definition is even more apparent when understood in the context of the statutory scheme of the WPA. Under current law, once an individual has made a

qualifying disclosure pursuant to 5 U.S.C. § 2302(b)(8), a *prima facie* case of whistleblower reprisal can be made by showing that a deciding agency official: a) knew of the disclosure; and b) an adverse action was taken within a reasonable time of the disclosure. *Kewley v. Department of Health & Human Serv.*, 153 F.3d 1357, 1362-62 (Fed. Cir. 1998) (citing 5 U.S.C. § 1221(e)(1)). Once the employee establishes this *prima facie* case, the burden shifts to the employing agency to show by clear and convincing evidence that it would have taken the adverse action regardless of the protected disclosure. *Kewley*, 153 F.3d at 1363.

Given the expanded definition of disclosure and the relatively light burden of establishing a *prima facie* case of reprisal under the knowledge/timing test, it would be exceedingly easy for employees to use whistleblowing as a defense to every adverse personnel action. Then the statutory structure of the WPA would require the agency to meet the much higher burden of demonstrating by clear and convincing evidence that it would have taken the adverse action, regardless of the disclosure. Thus, for all practical purposes, section 1(b)(1)(A) would transform the statutory standard that an agency must meet in sustaining almost every adverse action from a preponderance of the evidence, 5 U.S.C. § 7701(c)(1)(B), to the clear and convincing standard required by 5 U.S.C. § 1221(e)(2).

The ease with which a Federal employee would be able to establish a *prima facie* case of whistleblower reprisal, no matter how frivolous, would seriously impair the ability of Federal managers to effectively and efficiently manage the workforce. If Federal managers knew that it was likely that they would be subject to a charge of whistleblower reprisal every time that they took an adverse personnel action, they might hesitate to take any such action. Likewise, the very low standards that would be required to advance a whistleblower claim would vastly increase the number of such claims, obscure the claims of legitimate whistleblowers, and unduly burden the MSPB and the Federal Circuit.

Currently, the WPA does not cover disclosures that specifically are prohibited by law or disclosures of information that specifically are required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs. Subsection 1(b)(1)(B) would add 5 U.S.C. § 2302(b)(8)(C) to include this category of covered disclosures if the disclosure evidenced a reasonable belief of violation of law, rule, or regulation; gross mismanagement; gross waste of funds; abuse of authority; substantial and specific danger to public health or safety; or a false statement to Congress on an issue of material fact. The disclosure also would have to be made to a Member of Congress authorized to receive information of the type disclosed or to any employee of Congress having an appropriate security clearance and authorized to receive information of the type disclosed. The amendment would expand the scope of covered disclosures significantly and therefore substantially increase the potential exposure to litigation for Federal agencies as well as the staffing costs and other burdens associated with this issue.

## 2. Security Clearances

There are three significant provisions regarding security clearances. First, subsection 1(e)(1) of the bill would amend 5 U.S.C. § 2302(a)(2)(A) to add "a suspension, revocation, or other determination relating to a security clearance," to the definition of a personnel practice. Second, section 1(e)(2) (adding a new subparagraph (14) to 5 U.S.C. § 2302(b)) would amend the definition of prohibited personnel practices to include "conduct[ing] or caus[ing] to be conducted, an investigation of an employee or applicant for employment because of any activity protected under this section." Third, subsection 1(e)(3) of the bill would authorize the MSPB and the courts to review these security clearance decisions to determine whether a violation of 5 U.S.C. § 2302 (prohibited personnel practices) had occurred and, if so, to order certain relief. We have both general and technical objections to these provisions.

We strongly oppose these amendments because they would authorize the MSPB and the courts to review any determination relating to a security clearance – a prerogative left firmly within the Executive branch's discretion. In *Egan*, 484 U.S. 518 (1988), the Supreme Court explicitly rejected the proposition that the MSPB and the Federal Circuit could review the decision to revoke a security clearance. In doing so, the Court relied upon a number of premises, including: 1) decisions regarding security clearances are an inherently discretionary decision best left to the particular agency involved, not to be reviewed by non-expert bodies such as the MSPB and the courts; 2) review under the CSRA, which provides for a preponderance of the evidence standard, conflicts with the requirement that a security clearance should be given only when clearly consistent with the interests of the national security; and 3) that the President's power to make security clearance determinations is based in his constitutional role as Commander-in-Chief. See our constitutional objections at page 1, *supra*.

An example demonstrates one of the many fundamental problems with this bill's security clearance provisions. As we noted above, the burden of proof in CSRA cases is fundamentally incompatible with the standard for granting security clearances. This conflict is even more apparent in whistleblower cases. Under the WPA, a putative whistleblower establishes a *prima facie* case of whistleblower retaliation by establishing a protected disclosure and, under the knowledge/timing test, a personnel action taken within a certain period of time following the disclosure. Once the employee meets that minimal burden, the burden shifts to the agency to establish *by clear and convincing evidence* that it would have taken the action absent the protected disclosure.

Therefore, the bill would require in the security clearance context, that where individuals make protected disclosures (which, as we explain above, would include virtually every Federal employee under other amendments in this bill), the agency must justify its security clearance decision by the stringent standard of clear and convincing evidence. Thus, rather than awarding security clearances only where clearly consistent with the interests of national security, agencies would be permitted to deny or revoke them only upon the basis of clear and convincing evidence.



This standard would be shockingly inconsistent with national security, especially in these times of heightened security concerns.

Beyond these objections, the amendments are simply unnecessary. Currently, Executive Order 12968 requires all agencies to establish an internal review board to consider appeals of security clearance revocations. These internal boards provide sufficient protections for the subjects of the revocations, while, at the same time, preserving the authority of the Executive branch to make the necessary decisions. In any event, we are not aware of any pattern of abusing security clearance decisions to retaliate against whistleblowers. Thus, the drastic and potentially unconstitutional amendments subsections 1(e)(1) and 1(e)(3) would make are unwarranted.

We have other, more specific, objections to the bill. In defining the category of security clearance decisions that fall within a personnel action and, therefore, would be subject to review, subsection 1(e)(1) of the bill uses the phrase "suspension, revocation, or *other determination* relating to a security clearance" [emphasis added]. The phrase "other determination" is vague and conceivably could encompass such things as an initial investigation into whether a security clearance is warranted, the decision to upgrade or downgrade a clearance, or any other decision connected in any way with a security clearance. This broad language would convert nearly every action an agency takes with regard to a security clearance into a possible basis for a whistleblower charge.

In addition, section 1(e)(2), amending the definition of prohibited personnel practices to include "conduct[ing] or caus[ing] to be conducted, an investigation of an employee or applicant for employment because of any activity protected under this section," is overly broad. As drafted, the provision could be construed to restrict the scope of routine employment inquiries to prior employers, where the Government was a prior employer. This might be the case, for example, where an employee left government service after a whistleblower situation and several years later applied for employment with a different Government agency, necessitating a new background investigation. Section 1(e)(2) would lead to disputes over the scope and permissibility of such inquiries. Moreover, the bar seems to apply whether the claim of whistleblower status was upheld or not.

Finally, section 1(e)(3) of the bill contains language stating that the MSPB or any reviewing court "may not order the President to restore a security clearance." We presume this language was intended to alleviate concerns about the Executive branch prerogative with regard to security clearance determinations. However, the language, on its face, only prohibits the MSPB and reviewing court from ordering "the President" to "restore" a clearance. Conceivably, this language could be interpreted to allow the MSPB to order an agency head or lower official to restore the clearance. Likewise, it does not appear to limit the MSPB's authority to order other actions with regard to security clearances, for instance, to award an initial clearance, to order an upgrade, or to stop an investigation. It also is unclear to us why a narrow class of whistleblower reprisal cases merits the "expedited review" section 1(3)(e) would require and what that would mean in this context.

### 3. Confidential Advice on Making Disclosures to Congress

Subsection 1(j) would amend 5 U.S.C. § 2302(f) to require each agency to establish a procedure for providing confidential advice to employees on making lawful disclosures to Congress of information specifically required by law or Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs. This provision would place agencies in the odd and anomalous position of effectively encouraging their employees to disclose matters otherwise required by law to be kept secret. We oppose this provision.

### 4. Judicial Review

We object to section 1(k)(2) of the bill, which would grant the Office of Special Counsel the option to seek review of MSPB decisions by the regional courts of appeal rather than by the Federal Circuit. Review by the Federal Circuit promotes conformity in decisions and fosters uniformity in Federal personnel law. Granting the regional circuits jurisdiction to entertain appeals from the MSPB would undo Congress's sensible centralization of those appeals and further burden those already overburdened regional courts of appeal.

Since the enactment of the Federal Courts Improvement Act of 1982, the Federal Circuit has exercised exclusive jurisdiction to consider appeals from the MSPB in cases not involving discrimination. In those years, the court has developed substantial expertise and a well-defined body of law regarding Federal personnel matters that inures to the benefit of both the Federal Government and its employees. Moreover, the court's rules, which provide for more expedited and informal briefing in *pro se* cases provide an added benefit for Federal employees, many of whom choose to appeal the MSPB's decisions without the aid of an attorney.

Replacing the Federal Circuit's exclusive jurisdiction with review by the regional circuits would result in a fractured personnel system. Inevitably, conflicts among the circuits would arise as to the proper interpretation of the Federal personnel laws, so that an employee's rights and responsibilities would be determined by the geographic location of his or her place of employment. Not only is a non-uniform system undesirable, it could contribute to a loss of morale, as Federal employees would be treated differently depending upon where they lived. Inevitably, it would require the Supreme Court to intervene more often in Federal personnel matters to resolve inconsistencies among the circuits.

The CSRA and the Federal Courts Improvement Act resolved the problems of regional review. Considering the Federal Circuit's now substantial expertise, there simply is no good reason to revert to the old system. We have similar concerns about section 1(l) (amending 5 U.S.C. § 7703(b) and (d)).

## 5. Litigating Authority For The Special Counsel

Section 1(k) of the bill would expand the authority of the Special Counsel by authorizing her to seek review unilaterally in the United States Court of Appeals for the Federal Circuit in any case to which she was a party, *see* section 1(k)(2) (adding new 5 U.S.C. § 7703(e)(1)), and by granting her the authority to designate attorneys to appear upon her behalf in all courts except the Supreme Court, *see* section 1(k)(1) (adding new 5 U.S.C. § 1212(h)). Current law authorizes the Special Counsel to appear only before the MSPB. We oppose both of these changes.

Under current law, employees who are adversely affected by a decision of the MSPB have the right to appeal to the Court of Appeals for the Federal Circuit. *See* 5 U.S.C. § 7703(a). The Department of Justice represents the respondent Federal agencies in these appeals. Federal employing agencies do not possess the same right to appeal MSPB decisions adverse to them. OPM is the only Government agency that may appeal an MSPB decision and it may do so only after it has intervened in the MSPB proceeding to present its position and its director has determined that an MSPB decision rejecting OPM's position will have a "substantial impact" upon the administration of the civil service law. 5 U.S.C. § 7703(d). Moreover, once the director makes such a determination, OPM must seek authorization from the Justice Department's Solicitor General to file a petition for review. The Federal Circuit has discretion to grant or deny this petition. OPM is represented in the Federal Circuit by the Department of Justice.

Section 1(k)(2) of the bill would disrupt this carefully crafted scheme by authorizing the Special Counsel, without the approval of the Solicitor General, to petition the Federal Circuit for leave to appeal any adverse MSPB decision. The only limitation placed upon this right would be the requirement that the Special Counsel, if not a party to or intervenor in the matter before the MSPB, petition the MSPB for reconsideration of its decision before seeking review in the Federal Circuit.

Section 1(k)(1) would further erode centralized control over personnel litigation by authorizing the Office of the Special Counsel to represent itself in all litigation except litigation before the Supreme Court. This authority would be independent of the Department of Justice and could result in the Special Counsel litigating against other Executive branch agencies. This would usurp the Justice Department's traditional unifying role as the Executive branch's representative in court. We are unaware of any justification for eroding the Department's ability to fulfill its well-settled representative role.

Centralized control furthers a number of important policy goals, including the presentation of uniform positions on significant legal issues, the objective litigation of cases by attorneys unaffected by the parochial concerns of a single agency that might be inimical to the interests of the Government as a whole, and the facilitation of presidential supervision over Executive branch policies implicated in Government litigation. This policy benefits not only the

Government but also the courts and citizens who, in the absence of the policy, might be subjected to uncoordinated and inconsistent positions on the part of the Government.

## 6. Investigations

Subparagraph 1(e)(1)(B) of the bill would amend 5 U.S.C. § 2302(a)(2)(A) to include within WPA-covered personnel actions "an investigation of an employee or applicant for employment because of any activity protected under this section." Additionally, subparagraph 1(e)(2)(C) would amend 5 U.S.C. § 2302(b) to forbid Federal employees to "conduct, or cause to be conducted, an investigation of an employee or applicant for employment because of any activity protected under this section."

We are very troubled by the breadth of these provisions and the effect they could have on the ability of agencies to function. The amendments do not define an "investigation." Accordingly, it would appear that any type of inquiry by any agency, ranging from criminal investigation to routine background investigation for initial employment to investigation for determining eligibility for a security clearance to Inspector General investigation to management inquiries of potential wrongdoing in the workplace, all could be subject to challenge and litigation.

Conceivably, any time a supervisor suspected wrongdoing by an employee and determined to look into the matter, the "investigation" could be subject to challenge. Certainly, any time an Office of Inspector General, an Office of Professional Responsibility, or similar agency component began an investigation, the investigation immediately could become the subject of litigation. Through such litigation, employees would be able to delay or thwart any investigation into their own or others' wrongdoing. This result could adversely affect the ability and perhaps even the willingness of supervisors to examine wrongdoing – which clearly is not a beneficial outcome for the efficient and effective operation of agencies. Indeed, this provision could allow an employee to litigate an action that has not been proposed. Thus, even before any discipline had been proposed or any charges brought, the employee could attempt to short circuit any inquiry into the situation. In this connection, we note that the Equal Employment Opportunity Commission has prohibited the filing of a formal complaint on a "proposal to take a personnel action, or other preliminary step to taking a personnel action." See 29 C.F.R. § 1614.107(a)(5).

The CSRA is a careful balance between providing remedies for personnel actions that have been taken against Federal employees and permitting agencies to manage their workforces effectively. Subparagraphs 1(e)(1)(B) and 1(e)(2)(C) would upset that balance seriously, since an investigation is not an action against the employee but is a necessary government function for gathering facts about a wide range of matters so that informed decisions can be subsequently made.

Further, including conducting investigations and "causing them to be conducted" among the prohibited practices could decrease the willingness of any employee to report allegations of misconduct to an Office of Inspector General ("OIG"), which is generally responsible for conducting such investigations. Even the reporting of wrongdoing could be viewed as causing an investigation to be conducted and could subject not just investigators and managers but any employee who "causes" an investigation to be conducted to charges of committing a prohibited personnel practice.

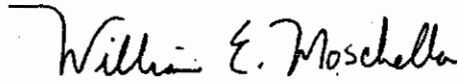
Moreover, the allegation of a prohibited personnel practice in the form of an investigation could result in an investigation by the Office of Special Counsel into an open criminal or administrative investigation and into open investigatory files, and then, pursuant to the OSC's statutory obligations, the reporting of that investigatory information to the complainant. Except in limited circumstances, open investigative files are not shared with other agencies or persons for several reasons, including the privacy interests of the subject and witnesses, and the protection of investigative techniques. Additionally, the Inspector General Act of 1978, as amended, 5 U.S.C. app. § 7(a), requires that the confidentiality of a Federal employee complainant be maintained "unless disclosure is unavoidable during the course of an investigation." Our concerns are amplified because of OSC's reporting of the progress of its investigation and its findings to the complainant. This reporting could compromise and undermine a legitimate law enforcement investigation.

## 7. Attorneys Fees

Section 1(g) of the bill would amend 5 U.S.C. § 1204(m)(1) to provide that, in disciplinary action cases, a prevailing employee could obtain attorney fees from the agency at which the prevailing party was employed rather than, as currently exists, from the agency proposing the disciplinary action against the employee. Essentially, this provision would shift the burden for attorney fees from the Office of Special Counsel, the agency responsible for pursuing disciplinary actions, to the prevailing party's employing agency. We object to this change for at least two reasons. First, one of the general policies underlying fee-shifting provisions against the Government is ensuring that the Government acts responsibly. By shifting the burden from the agency responsible for taking disciplinary actions – the Special Counsel – to the employing agency, this amendment would eliminate this important check on the Special Counsel in considering which actions to pursue because even if the Special Counsel took an unjustified action, it will not have to bear the attorney fees. Second, this amendment is patently unfair to the employing agencies, which might disagree with the action the Special Counsel was pursuing but nevertheless would be responsible for any fees. Indeed, it is not uncommon that an agency will refuse to take a disciplinary action that is proposed by the Special Counsel, agreeing with a particular employee that no wrongdoing had been committed. If the employee hired an attorney and successfully defended himself against the Special Counsel before the MSPB or the Federal Circuit, the employing agency – who disagreed with the Special Counsel's actions – would be required to pay the fees.

Thank you for the opportunity to present our views. Please do not hesitate to call upon us if we may be of additional assistance. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to submission of this report.

Sincerely,

A handwritten signature in cursive script that reads "William E. Moschella".

William E. Moschella  
Assistant Attorney General

cc: The Honorable Daniel K. Akaka  
Ranking Minority Member



U.S. Department of Justice

Office of Legislative Affairs

---

Washington, D.C. 20530

October 8, 2004

The Honorable Susan M. Collins  
Chairman  
Committee on Governmental Affairs  
United States Senate  
Washington, D.C. 20510

Dear Madam Chairman:

This presents the views of the Department of Justice on S. 2628, the "Federal Employee Protection of Disclosures Act." While we understand the important public interest in protecting whistleblowers, we must oppose this bill very strongly.

S. 2628 would make a number of significant and extremely undesirable changes to the Whistleblower Protection Act ("WPA") and the Civil Service Reform Act ("CSRA"). Among other things, the bill would permit, for the first time, the Merit Systems Protection Board ("MSPB") and the courts to review the Executive branch's decisions regarding security clearances. It would provide new protections for the unauthorized disclosure of classified information. It would make sweeping changes to the WPA, including a vast expansion of the definition of a "protected disclosure." It would alter the carefully crafted scheme for judicial review of decisions of the MSPB, which is set forth in the CSRA. It would grant the Office of Special Counsel independent litigating authority. S. 2628 is burdensome, unnecessary, and unconstitutional. Rather than promote and protect genuine disclosures of matters of real public concern, it would provide a legal shield for unsatisfactory employees. *See, e.g.,* S. Rep. No. 100-413, at 15 (1988) ("The Committee does not intend that employees who are poor performers escape sanction by manufacturing a claim of whistleblowing"); S. Rep. No. 95-969, at 8, *reprinted in* 1978 U.S.S.C.A.N. 2723, 2730-31 ("Nor would the bill protect employees who claim to be whistle blowers in order to avoid adverse action based on inadequate performance").

The Justice Department testified in opposition to S. 1358, the previous version of this legislation, and submitted responses to questions for the record further explaining our opposition to aspects of that bill. While S. 2628 reflects some changes from S. 1358, the basic flaws of that prior legislation remain. For example, while the Office of Special Counsel ("OSC") is given

amicus status rather than party status in appeals under S. 2628, the bill directs that courts allow OSC's participation as an amicus. This kind of participation is likely to reveal a split in the positions of two agencies of the Executive branch. Additionally, there are very significant constitutional problems with the bill.

### **I. Constitutional Concerns**

We have several constitutional concerns about the bill. In particular, we strongly recommend that subparagraphs 1(b)(3), 1(e)(2), and 1(e)(3), and subsection 1(k) of the bill be deleted.

Section 1(b)(3) would add subparagraph (C) to 5 U.S.C. § 2302(b)(8). Subsection (C) would prohibit a "personnel action"<sup>1</sup> against a covered Executive branch employee or applicant for employment who disclosed to any Member or employee of Congress, who is "authorized to receive information of the type disclosed," "information required by law or Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs." The prohibition would apply where the employee "reasonably believes" the information is "direct and specific evidence" of "any violation of any law," of "gross mismanagement, a gross waste of funds, an abuse of authority, . . . a substantial and specific danger to public health or safety," or "a false statement to Congress."

Consistent with our longstanding views, we strongly oppose this provision as unconstitutional. In 1998, the Department objected to S. 1668, a bill similar to S. 2628, that would have required the President to inform employees of covered Federal agencies that their disclosure to Congress of classified information that the employee reasonably believed provided direct and specific evidence of misconduct (including violations of law) is not prohibited. *See Statement of Randolph Moss, Deputy Assistant Attorney General, Office of Legal Counsel, Before the House Permanent Select Committee on Intelligence, Concerning Whistleblower Protections for Classified Disclosures* (May 20, 1998) ("Moss testimony"). The Department testified that S. 1668 "would deprive the President of his authority to decide, based on the national interest, how, when and under what circumstances particular classified information should be disclosed to Congress. This is an impermissible encroachment on the President's ability to carry out core executive functions. In the congressional oversight context, as in all others, the decision whether and under what circumstances to disclose classified information must be made by someone who is acting on the official authority of the President and who is ultimately responsible to the President. The constitution does not permit Congress to authorize

---

<sup>1</sup>The prohibition would include discipline and also including, pursuant to subparagraph 1(e)(1)(B), implementing or enforcing a nondisclosure agreement, suspending a security clearance, or conducting certain investigations.



subordinate executive branch employees to bypass these orderly procedures for review and clearance by vesting them with a unilateral right to disclose classified information – even to Members of Congress.” *Id.* at 16.

Like S. 1668, S. 2628 would permit any covered Executive branch employee (or applicant) to disclose to Congress classified national security information without receiving official authorization to do so. Existing law merely precludes “personnel actions” against covered employees who make such disclosures to the Special Counsel or to the Inspector General of an agency, *see* 5 U.S.C. 2302(b)(8)(B), who are both Executive branch officials. By contrast, S. 2628 would allow any covered employee with access to classified information to go directly to Congress, thereby unilaterally circumventing the process by which the Executive branch and Legislative branch accommodate each other’s interests in sensitive information. *See* 13 Op. O.L.C. at 157-61 (discussing accommodation process). Congress may not vest lower-ranking personnel in the Executive branch with a “right” to furnish national security or other privileged information to Congress without receiving official authorization to do so.

For similar reasons, we recommend that subparagraphs 1(e)(2) and 1(k) of the bill be deleted. These sections purport to dictate and micromanage the specific content of nondisclosure agreements applicable to Executive branch employees (and contractors), in violation of the President’s authority “to decide, based on the national interest, how, when and under what circumstances particular classified information should be disclosed.” Moss Testimony at 16.

Finally, we recommend deleting subparagraph 1(e)(3) of the bill. This section would require the Merit Systems Protection Board (“MSPB”) or any reviewing court, in any appeal relating to a security-clearance determination, to review and decide whether a security-clearance determination was made because the employee disclosed information, including national security information, that the bill permits the employee to disclose. This section unconstitutionally intrudes on “the President’s constitutional responsibility to protect certain information.” 13 Op. O.L.C. at 254. A security-clearance decision requires “a sensitive and inherently discretionary judgment call” that the Constitution vests in the President “quite apart from any explicit congressional grant.” *Dep’t of the Navy v. Egan*, 484 U.S. 518, 527 (1988) (concluding that the MSPB lacked statutory authority to review the substance of an underlying decision to deny or revoke a security clearance); *see also id.* (The President’s “authority to classify and control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to occupy a position in the Executive Branch that will give that person access to such information flows primarily from the [Commander-in-Chief Clause’s] investment of power in the President.”); *id.* (“The authority to protect [national security] information falls on the President as head of the Executive Branch and as Commander in Chief.”). As the Supreme Court has concluded, “For ‘reasons . . . too obvious to call for enlarged discussion,’ *CIA v. Sims*, 471 U.S. 159, 170 (1985), the protection of classified information must be committed to the broad discretion of the agency responsible, and this must include broad discretion to determine

who may have access to it. Certainly, it is not reasonably possible for an outside nonexpert body to review the substance of such a judgment . . .” *Egan*, 484 U.S. at 528.

## II. Other Concerns

### 1. Expanded Definition Of Protected Disclosure

Subsection 1(b)(1)(A) of the bill would broaden the definition of “protected disclosure” by amending 5 U.S.C. § 2302(b)(8)(A) to state:

any disclosure of information by an employee or applicant, *without restriction to time, place, form, motive, context, or prior disclosure made to any person by an employee or applicant, including a disclosure made in the ordinary course of an employee's duties* that the employee or applicant reasonably believes is evidence of

(i) *any violation* of any law, rule, or, regulation, or

(ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety. [emphasis added]

This amendment appears intended to override or supersede a series of decisions by the United States Court of Appeals for the Federal Circuit that defined the scope of disclosures covered by section 2302(b)(8). *See, e.g., Horton v. Dep't of Navy*, 66 F.3d 279, 282 (Fed. Cir. 1995) (complaints to wrongdoers are not protected whistleblowing); *Willis v. Dep't of Agriculture*, 141 F.3d 1139, 1143-44 (Fed. Cir. 1998) (ordinary work disagreements not protected disclosures, nor are disclosures made during the course of performing ordinary job duties); *Meuwissen v. Dep't of the Interior*, 234 F.3d 9, 12-14 (Fed. Cir. 2000) (discussion of matters already known does not constitute a covered disclosure); *LaChance v. White*, 174 F.3d 1378, 1381 (Fed. Cir. 1999) (in determining whether a disclosure is covered, the Board should consider the motives of the employee making the disclosure). The Federal Circuit precedent was useful to Federal agencies because it insulated them from having to defend against potentially burdensome whistleblower litigation involving no more than workplace disagreements, complaints by disgruntled employees, or matters that never were, in any real sense, “disclosed” to any individuals or organizations having any authority to address the disclosures.

The expanded definition in subsection 1(b)(1)(A) would upset the delicate balance between whistleblower protection and the ability of Federal managers to manage the workforce. The WPA already provides adequate protection for legitimate whistleblowers. The proposed expansive definition has the potential to convert any disagreement or contrary interpretation of a

law, no matter how trivial or frivolous, into a whistleblower disclosure. It will not provide further protection to those with legitimate claims, who are covered by the existing law. It simply will increase the number of frivolous claims of whistleblower reprisal. Such an increase in the number of frivolous claims would impose an unwarranted burden upon Federal managers and, ultimately, the MSPB and the Federal Judiciary.

The Federal Circuit appropriately has recognized that the purposes of the WPA must be taken into account in determining whether a disclosure is one protected by the WPA. *Willis v. Department of Agriculture*, 141 F.3d 1139, 1143 (Fed. Cir. 1998) (observing that “[t]he purpose of the WPA is to encourage government personnel to disclose government wrongdoing to persons who may be in a position to remedy the problem without fearing retaliatory action by their supervisors or those who might be harmed by the disclosures.”). Accordingly, the court in *Willis* recognized that expressing disagreement with a supervisor's decision to that supervisor was not the type of disclosure protected by the WPA because it was not reporting the supervisor's wrongdoing to anyone in a position to take action. *Id.* Moreover, the court found that the WPA was not intended to protect reports of violations of laws, rules, or regulations that an employee made as a part of his everyday job responsibilities. *Id.* at 1143-44.

These limitations are reasonable and serve to further the purpose of the WPA to protect legitimate whistleblowers. By prohibiting the consideration of “time, place, form, motive, context” and including the performance of one’s job duties in the definition of “disclosures,” the bill converts every Federal employee into a whistleblower. Nearly every Federal employee will, sometime during the course of his or her career, disagree with a statement or interpretation made by a supervisor, or during the course of performing his or her everyday responsibilities, report an error that may demonstrate a violation of a law, rule, or regulation. Without the ability to take the context – the time, the place, the motive – of the alleged disclosure into account, even trivial or *de minimis* matters would become elevated to the status of protected disclosures. *Cf. Herman v. Department of Justice*, 193 F.3d 1375, 1378-79 (Fed. Cir. 1999) (concluding that the WPA was not intended to apply to trivial matters). This provision would undermine the effectiveness of the WPA.

The danger of this expanded definition is even more apparent when understood in the context of the statutory scheme of the WPA. Under current law, once an individual has made a qualifying disclosure pursuant to 5 U.S.C. § 2302(b)(8), a *prima facie* case of whistleblower reprisal can be made by showing that a deciding agency official: a) knew of the disclosure; and b) an adverse action was taken within a reasonable time of the disclosure. *Kewley v. Department of Health & Human Serv.*, 153 F.3d 1357, 1362-62 (Fed. Cir. 1998) (citing 5 U.S.C. § 1221(e)(1)). Once the employee establishes this *prima facie* case, the burden shifts to the employing agency to show by clear and convincing evidence that it would have taken the adverse action regardless of the protected disclosure. *Kewley*, 153 F.3d at 1363.

Given the expanded definition of disclosure and the relatively light burden of establishing a *prima facie* case of reprisal under the knowledge/timing test, it would be exceedingly easy for employees to use whistleblowing as a defense to every adverse personnel action. Then the statutory structure of the WPA would require the agency to meet the much higher burden of demonstrating by clear and convincing evidence that it would have taken the adverse action, regardless of the disclosure. Thus, for all practical purposes, section 1(b)(1)(A) would transform the statutory standard that an agency must meet in sustaining almost every adverse action from a preponderance of the evidence, 5 U.S.C. § 7701(c)(1)(B), to the clear and convincing standard required by 5 U.S.C. § 1221(e)(2).

The ease with which a Federal employee would be able to establish a *prima facie* case of whistleblower reprisal, no matter how frivolous, would seriously impair the ability of Federal managers to effectively and efficiently manage the workforce. If Federal managers knew that it was likely that they would be subject to a charge of whistleblower reprisal every time that they took an adverse personnel action, they might hesitate to take any such action. Likewise, the very low standards that would be required to advance a whistleblower claim would vastly increase the number of such claims, obscure the claims of legitimate whistleblowers, and unduly burden the MSPB and the Federal Circuit.

Currently, the WPA does not cover disclosures that specifically are prohibited by law or disclosures of information that specifically are required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs. Subsection 1(b)(3) would add 5 U.S.C. § 2302(b)(8)(C) to include this category of covered disclosures if the disclosure evidenced a reasonable belief of violation of law, rule, or regulation; gross mismanagement; gross waste of funds; abuse of authority; substantial and specific danger to public health or safety; or a false statement to Congress on an issue of material fact. The disclosure also would have to be made to a Member of Congress authorized to receive information of the type disclosed or to any employee of Congress having an appropriate security clearance and authorized to receive information of the type disclosed. The amendment would expand the scope of covered disclosures significantly and therefore substantially increase the potential exposure to litigation for Federal agencies as well as the staffing costs and other burdens associated with this issue.

## **2. Security Clearances**

There are three significant provisions regarding security clearances. First, subsection 1(e)(1) of the bill would amend 5 U.S.C. § 2302(a)(2)(A) to add “a suspension, revocation, or other determination relating to a security clearance,” to the definition of a personnel practice. Second, section 1(e)(2) (adding a new subparagraph (14) to 5 U.S.C. § 2302(b)) would amend the definition of prohibited personnel practices to include “conduct[ing] or caus[ing] to be conducted, an investigation, other than any ministerial or nondiscretionary fact finding activities necessary for the agency to perform its mission, of an employee or applicant for employment

because of any activity protected under this section.” Third, subsection 1(e)(3) of the bill would authorize the MSPB and the courts to review these security clearance decisions to determine whether a violation of 5 U.S.C. § 2302 (prohibited personnel practices) had occurred and, if so, to order certain relief. We have both general and technical objections to these provisions.

We strongly oppose these amendments because they would authorize the MSPB and the courts to review any determination relating to a security clearance – a prerogative left firmly within the Executive branch's discretion. See our constitutional objections, *supra*. This conflict is even more apparent in whistleblower cases. Under the WPA, a putative whistleblower establishes a *prima facie* case of whistleblower retaliation by establishing a protected disclosure and, under the knowledge/timing test, a personnel action taken within a certain period of time following the disclosure. Once the employee meets that minimal burden, the burden shifts to the agency to establish *by clear and convincing evidence* that it would have taken the action absent the protected disclosure.

Therefore, the bill would require in the security clearance context, that where individuals make protected disclosures (which, as we explain above, would include virtually every Federal employee under other amendments in this bill), the agency must justify its security clearance decision by the stringent standard of clear and convincing evidence. Thus, rather than awarding security clearances only where clearly consistent with the interests of national security, agencies would be permitted to deny or revoke them only upon the basis of clear and convincing evidence. This standard would be shockingly inconsistent with national security, especially in these times of heightened security concerns.

Beyond these objections, the amendments are simply unnecessary. Currently, Executive Order 12968 requires all agencies to establish an internal review board to consider appeals of security clearance revocations. These internal boards provide sufficient protections for the subjects of the revocations, while, at the same time, preserving the authority of the Executive branch to make the necessary decisions. In any event, we are not aware of any pattern of abusing security clearance decisions to retaliate against whistleblowers. Thus, the drastic and potentially unconstitutional amendments subsections 1(e)(1) and 1(e)(3) would make are unwarranted.

We have other, more specific, objections to the bill. In defining the category of security clearance decisions that fall within a personnel action and, therefore, would be subject to review, subsection 1(e)(1) of the bill uses the phrase “suspension, revocation, or *any other determination relating to a security clearance or any other access determination by a covered agency*” [emphasis added]. Although the phrase “other determination” remains vague, the remainder of the provision, “or any other access determination by a covered agency,” is so broad as to encompass such things as an initial investigation into whether a security clearance is warranted, the decision to upgrade or downgrade a clearance, or any other decision connected in any way

with a security clearance. This broad language would convert nearly every action an agency takes with regard to a security clearance into a possible basis for a whistleblower charge.

In addition, subparagraph 1(e)(2), amending the definition of prohibited personnel practices to include “conduct[ing] or caus[ing] to be conducted, an investigation, other than any ministerial or nondiscretionary fact finding activities necessary for the agency to perform its mission, of an employee or applicant for employment because of any activity protected under this section,” remains somewhat vague and potentially overly broad. Although this provision appears intended to allow the Government to conduct certain routine employment inquiries regarding current and prospective employees, it still will lead to disputes over the scope and permissibility of such inquiries.

Finally, section 1(e)(3) of the bill contains language stating that the MSPB or any reviewing court “may not order the President to restore a security clearance.” We presume this language was intended to alleviate concerns about the Executive branch prerogative with regard to security clearance determinations. However, the language, on its face, only prohibits the MSPB and reviewing court from ordering “the President” to “restore” a clearance. Conceivably, this language could be interpreted to allow the MSPB to order an agency head or lower official to restore the clearance. Likewise, it does not appear to limit the MSPB’s authority to order other actions with regard to security clearances, for instance, to award an initial clearance, to order an upgrade, or to stop an investigation. It also is unclear to us why a narrow class of whistleblower reprisal cases merits the “expedited review” section 1(e)(3) would require and what that would mean in this context.

### **3. Confidential Advice on Making Disclosures to Congress**

Subsection 1(m) would amend 5 U.S.C. § 2302(f) to require each agency to establish a procedure for providing confidential advice to employees on making lawful disclosures to Congress of information specifically required by law or Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs. This provision would place agencies in the odd and anomalous position of effectively encouraging their employees to disclose matters otherwise required by law to be kept secret. We oppose this provision.

### **4. Investigations**

Subparagraph 1(e)(1)(B) of the bill would amend 5 U.S.C. § 2302(a)(2)(A) to include within WPA-covered personnel actions “an investigation, other than any ministerial or nondiscretionary fact finding activities necessary for the agency to perform its mission, of an employee or applicant for employment because of any activity protected under this section.” Additionally, subparagraph 1(e)(2)(C) would amend 5 U.S.C. § 2302(b) to add new subparagraph (14), forbidding Federal employees to “conduct, or cause to be conducted, an investigation, other

than any ministerial or nondiscretionary fact finding activities necessary for the agency to perform its mission, of an employee or applicant for employment because of any activity protected under this section.”

We are very troubled by the breadth of these provisions and the effect they could have on the ability of agencies to function. The amendments do not define adequately an “investigation.” Accordingly, it would appear that any type of inquiry by any agency, ranging from criminal investigation to investigation for determining eligibility for a security clearance to Inspector General investigation to management inquiries of potential wrongdoing in the workplace, all could be subject to challenge and litigation.

Conceivably, any time a supervisor suspected wrongdoing by an employee and determined to look into the matter, the “investigation” could be subject to challenge. Certainly, any time an Office of Inspector General, an Office of Professional Responsibility, or similar agency component began an investigation, the investigation immediately could become the subject of litigation. Through such litigation, employees would be able to delay or thwart any investigation into their own or others’ wrongdoing. This result could adversely affect the ability and perhaps even the willingness of supervisors to examine wrongdoing – which clearly is not a beneficial outcome for the efficient and effective operation of agencies. Indeed, this provision could allow an employee to litigate an action that has not been proposed. Thus, even before any discipline had been proposed or any charges brought, the employee could attempt to short circuit any inquiry into the situation. In this connection, we note that the Equal Employment Opportunity Commission has prohibited the filing of a formal complaint on a “proposal to take a personnel action, or other preliminary step to taking a personnel action.” See 29 C.F.R. § 1614.107(a)(5).

The CSRA is a careful balance between providing remedies for personnel actions that have been taken against Federal employees and permitting agencies to manage their workforces effectively. Subparagraphs 1(e)(1)(B) and 1(e)(2)(C) would upset that balance seriously, since an investigation is not an action against the employee but is a necessary government function for gathering facts about a wide range of matters so that informed decisions can be subsequently made.

Further, including conducting investigations and “causing them to be conducted” among the prohibited practices could decrease the willingness of any employee to report allegations of misconduct to an Office of Inspector General (“OIG”), which is generally responsible for conducting such investigations. Even the reporting of wrongdoing could be viewed as causing an investigation to be conducted and could subject not just investigators and managers but any employee who “causes” an investigation to be conducted to charges of committing a prohibited personnel practice.

Moreover, the allegation of a prohibited personnel practice in the form of an investigation could result in an investigation by the Office of Special Counsel into an open criminal or administrative investigation and into open investigatory files, and then, pursuant to the OSC's statutory obligations, the reporting of that investigatory information to the complainant. Except in limited circumstances, open investigative files are not shared with other agencies or persons for several reasons, including the privacy interests of the subject and witnesses, and the protection of investigative techniques. Additionally, the Inspector General Act of 1978, as amended, 5 U.S.C. app. § 7(a), requires that the confidentiality of a Federal employee complainant be maintained "unless disclosure is unavoidable during the course of an investigation." Our concerns are amplified because of OSC's reporting of the progress of its investigation and its findings to the complainant. This reporting could compromise and undermine a legitimate law enforcement investigation.

## **5. Attorneys Fees**

Section 1(g) of the bill would amend 5 U.S.C. § 1204(m)(1) to provide that, in disciplinary action cases, a prevailing employee could obtain attorneys fees from the agency at which the prevailing party was employed rather than, as currently exists, from the agency proposing the disciplinary action against the employee. Essentially, this provision would shift the burden for attorneys fees from the Office of Special Counsel, the agency responsible for pursuing disciplinary actions, to the prevailing party's employing agency. We object to this change for at least two reasons. First, one of the general policies underlying fee-shifting provisions against the Government is ensuring that the Government acts responsibly. By shifting the burden from the agency responsible for taking disciplinary actions – the Special Counsel – to the employing agency, this amendment would eliminate this important check on the Special Counsel in considering which actions to pursue because even if the Special Counsel took an unjustified action, it will not have to bear the attorneys fees. Second, this amendment is patently unfair to the employing agencies, which might disagree with the action the Special Counsel was pursuing but nevertheless would be responsible for any fees. Indeed, it is not uncommon that an agency will refuse to take a disciplinary action that is proposed by the Special Counsel, agreeing with a particular employee that no wrongdoing had been committed. If the employee hired an attorney and successfully defended himself against the Special Counsel before the MSPB or the Federal Circuit, the employing agency – who disagreed with the Special Counsel's actions – would be required to pay the fees.

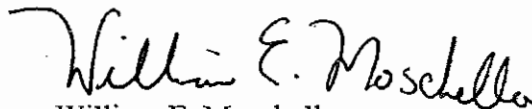
We recognize that certain agencies (*e.g.*, the FBI, the CIA, and the National Security Agency) are exempt from the statute (*i.e.*, they can discipline employees for whistleblowing). However, the Departments of Homeland Security, Justice, State and Defense (all of which deal with classified information on a regular basis) are not exempt unless the President specifically makes them exempt prior to a whistleblowing event.



The Honorable Susan M. Collins  
Page 11

Thank you for the opportunity to present our views. Please do not hesitate to call upon us if we may be of additional assistance. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,

A handwritten signature in black ink that reads "William E. Moschella". The signature is written in a cursive style with a large, sweeping initial "W".

William E. Moschella  
Assistant Attorney General

cc: The Honorable Joseph I. Lieberman  
Ranking Minority Member



U.S. Department of Justice

Office of Legislative Affairs

---

Washington, D.C. 20530

April 12, 2005

The Honorable Susan M. Collins  
Chairman  
Committee on Homeland Security  
and Governmental Affairs  
United States Senate  
Washington, D.C. 20510

Dear Madam Chairman:

This presents the views of the Department of Justice on S. 494, the "Federal Employee Protection of Disclosures Act." While we understand the important public interest in protecting whistleblowers, we must oppose this bill very strongly. This position is consistent with our opposition to an identical bill in the previous Congress, S. 2628.

S. 494 would make a number of significant and extremely undesirable changes to the Whistleblower Protection Act ("WPA") and the Civil Service Reform Act ("CSRA"). Among other things, the bill would permit, for the first time, the Merit Systems Protection Board ("MSPB") and the courts to review the Executive branch's decisions regarding security clearances. It would provide new protections for the unauthorized disclosure of classified information. It would make sweeping changes to the WPA, including a vast expansion of the definition of a "protected disclosure." It would alter the carefully crafted scheme for judicial review of decisions of the MSPB, which is set forth in the CSRA. It would grant the Office of Special Counsel independent litigating authority. S. 494 is burdensome, unnecessary, and unconstitutional. Rather than promote and protect genuine disclosures of matters of real public concern, it would provide a legal shield for unsatisfactory employees. *See, e.g.,* S. Rep. No. 100-413, at 15 (1988) ("The Committee does not intend that employees who are poor performers escape sanction by manufacturing a claim of whistleblowing"); S. Rep. No. 95-969, at 8, *reprinted in* 1978 U.S.S.C.A.N. 2723, 2730-31 ("Nor would the bill protect employees who claim to be whistle blowers in order to avoid adverse action based on inadequate performance").

During the previous Congress, the Justice Department testified in opposition to another, previous version of this legislation, S. 1358, and submitted responses to questions for the record

further explaining our opposition to aspects of that bill. While S. 494 reflects some changes from S. 1358, the basic flaws of that prior legislation remain. For example, while the Office of Special Counsel ("OSC") is given *amicus* status rather than party status in appeals under S. 494, the bill directs that courts allow OSC's participation as an amicus. This kind of participation is likely to reveal a split in the positions of two agencies of the Executive branch. In this area in particular, it is important for the Administration to speak with one voice. Additionally, there are very significant constitutional problems with the bill.

### I. Constitutional Concerns

We have several constitutional concerns about the bill. In particular, we strongly recommend that subparagraphs 1(b)(3), 1(e)(2), and 1(e)(3), and subsection 1(k) of the bill be deleted.

Section 1(b)(3) would add subparagraph (C) to 5 U.S.C. § 2302(b)(8). Subparagraph (C) would prohibit a "personnel action"<sup>1</sup> against a covered Executive branch employee or applicant for employment who disclosed to any Member or employee of Congress, who is "authorized to receive information of the type disclosed," "information required by law or Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs." The prohibition would apply where the employee "reasonably believes" the information is "direct and specific evidence" of "any violation of any law," of "gross mismanagement, a gross waste of funds, an abuse of authority, . . . a substantial and specific danger to public health or safety," or "a false statement to Congress."

Consistent with our longstanding views, we strongly oppose this provision as unconstitutional. Indeed, just last year, we objected strenuously to an identical bill, S. 2628; and in 1998, the Department objected to S. 1668, a bill similar to S. 494, that would have required the President to inform employees of covered Federal agencies that their disclosure to Congress of classified information that the employee reasonably believed provided direct and specific evidence of misconduct (including violations of law) is not prohibited. *See Statement of Randolph Moss, Deputy Assistant Attorney General, Office of Legal Counsel, Before the House Permanent Select Committee on Intelligence, Concerning Whistleblower Protections for Classified Disclosures* (May 20, 1998) ("Moss testimony"). The Department testified that S. 1668

would deprive the President of his authority to decide, based on the national interest, how, when and under what circumstances particular classified information should be disclosed to Congress. This is an impermissible

---

<sup>1</sup>The prohibition would include discipline and also including, pursuant to subparagraph 1(e)(1)(B), implementing or enforcing a nondisclosure agreement, suspending a security clearance, or conducting certain investigations.

encroachment on the President's ability to carry out core executive functions. In the congressional oversight context, as in all others, the decision whether and under what circumstances to disclose classified information must be made by someone who is acting on the official authority of the President and who is ultimately responsible to the President. The constitution does not permit Congress to authorize subordinate executive branch employees to bypass these orderly procedures for review and clearance by vesting them with a unilateral right to disclose classified information – even to Members of Congress.

*Id.* at 16.

Like S. 1668, S. 494 would permit any covered Executive branch employee (or applicant) to disclose to Congress classified national security information without receiving official authorization to do so. Existing law merely precludes “personnel actions” against covered employees who make such disclosures to the Special Counsel or to the Inspector General of an agency, *see* 5 U.S.C. 2302(b)(8)(B), who are both Executive branch officials. By contrast, S. 494 would allow any covered employee with access to classified information to go directly to Congress, thereby unilaterally circumventing the process by which the Executive branch and Legislative branch accommodate each other's interests in sensitive information. *See* 13 Op. O.L.C. at 157-61. As we have explained, “[t]he process of accommodation requires that each branch explain to the other why it believes its needs to be legitimate. . . . If either branch has a reason for needing to obtain or withhold information, it should be able to express it.” *Id.* at 159. Congress may not vest lower-ranking personnel in the Executive branch with a “right” to furnish national security or other privileged information to Congress without receiving official authorization to do so.

This provision would unconstitutionally deprive the President of his authority to decide, based on the national interest, how, when, and under what circumstances particular classified information should be disclosed to Congress. The Constitution not only generally establishes the President as the head of the Executive branch but also makes him Commander in Chief of all military forces, the sole organ of America's foreign affairs, and the officer in the Government with the express duty (and corresponding authority) to take care that the laws are faithfully executed. The President's authority to classify and control access to national security information in the Executive branch flows directly from these powers, as both this Department and the courts have long recognized. *See Dep't of the Navy v. Egan*, 484 U.S. 518, 527 (1988); *see also New York Times Co. v. United States*, 403 U.S. 713, 729-30 (1971) (Stewart, J., concurring) (“[I]t is clear to me that it is the constitutional duty of the Executive – as a matter of sovereign prerogative and not as a matter of law as the courts know law – through the promulgation and enforcement of executive regulations, to protect the confidentiality necessary to carry out its responsibilities in the fields of international relations and national defense.”); *Common Legislative Encroachments on Executive Branch Authority*, 13 Op. O.L.C. 248, 254 (1989) (describing “the President's constitutional responsibility to protect certain information”).

In *Department of the Navy v. Egan*, the Supreme Court expressly recognized the constitutional foundation of the President's authority to protect national-security information:

The President, after all, is the "Commander in Chief of the Army and Navy of the United States." U.S. Const., Art. II, § 2. His authority to classify and control access to information bearing on national security . . . *flows primarily from this constitutional investment of power in the President* and exists quite apart from any explicit congressional grant. . . . The authority to protect such information falls on the President as head of the Executive Branch and as Commander in Chief.

484 U.S. at 527 (emphasis added); *see also, e.g., Hill v. Dep't of the Air Force*, 844 F.2d 1407, 1410 (10th Cir. 1988) (acknowledging that the President's authority to protect national security information is constitutional based).<sup>2</sup>

The recognition of this authority stretches back to the earliest days of the Republic and across many partisan divides. *See History of Refusals by Executive Branch Officials to Provide Information Demanded by Congress*, 6 Op. O.L.C. 751 (1982) (compiling historical examples of cases in which the President withheld from Congress information the release of which he determined could jeopardize national security); *Congressional Requests for Confidential Executive Branch Information*, 13 Op. O.L.C. 153, 154 (1989) (stating that privilege "has been asserted by numerous Presidents from the earliest days of our nation"). Indeed, the Department's present position amounts to a reiteration of that taken by the Department in the Clinton Administration. *See, e.g., Statement of Randolph Moss, Deputy Assistant Attorney General*,

---

<sup>2</sup>Although *Egan* states that "unless Congress specifically has provided otherwise, courts traditionally have been reluctant to intrude upon the authority of the Executive in military and national security affairs," this language, when read in context, merely confirms that in the areas of foreign policy and national security courts have shown deference to *both* elected branches. *See Egan*, 484 U.S. at 530. Indeed, each of the five cases that the *Egan* Court cites following the quoted language supports judicial deference to both the President and Congress. It hardly follows from this tradition of judicial deference to the political branches that the Court is obliquely suggesting a power of Congress to usurp the President's longstanding power over national-security information. Not one of these cases addresses – much less supports – such congressional intrusion. *Egan* explicitly recognized the "constitutional investment of power in the President," which "exists quite apart from any explicit congressional grant," "to classify and control access to information bearing on national security." *Id.* at 527. That the "Constitution nowhere expressly states that the President, or the executive branch generally, enjoys a privilege against disclosing information requested by . . . the legislative branch" does not diminish this authority, which "is a necessary corollary of the executive function vested in the President by Article II of the Constitution." 13 Op. O.L.C. at 154; *see also United States v. Nixon*, 418 U.S. 683, 706-07 n.16, 711 (1974) (specifically holding that executive privilege is constitutionally based even though not expressly provided for in the Constitution).

*Office of Legal Counsel, Department of Justice, Before the House Permanent Select Committee on Intelligence, Concerning Whistleblower Protections for Classified Disclosures* (May 20, 1998).

The Executive branch remains committed to accommodating Congress's legitimate oversight needs in ways that are consistent with the Executive branch's constitutional responsibilities. However, subparagraph 1(b)(3) is unnecessary to satisfy Congress's interest in receiving information that enables it to carry out its oversight responsibilities. A process exists by which this has been and may be done. See 13 Op. O.L.C. at 157-61 (describing accommodation process). Subparagraph 1(b)(3) would circumvent this longstanding process unilaterally by allowing any covered employee with access to classified information to go directly to Congress. The process of dynamic compromise between the branches, whereby each branch seeks an optimal accommodation by evaluating the needs of the other, cannot function where every covered employee of the Executive branch is vested with the right to decide for himself or herself, without any official authorization, those disclosures that are appropriate.

For similar reasons, we recommend that subparagraphs 1(e)(2) and 1(k) of the bill be deleted. These sections purport to dictate and micromanage the specific content of nondisclosure agreements applicable to Executive branch employees (and contractors), in violation of the President's authority "to decide, based on the national interest, how, when and under what circumstances particular classified information should be disclosed." Moss Testimony at 16.

Finally, we recommend deleting subparagraph 1(e)(3) of the bill. This section would require the Merit Systems Protection Board ("MSPB") or any reviewing court, in any appeal relating to a security-clearance determination, to review and decide whether a security-clearance determination was made because the employee disclosed information, including national security information, that the bill permits the employee to disclose. This section unconstitutionally intrudes on "the President's constitutional responsibility to protect certain information." 13 Op. O.L.C. at 254. A security-clearance decision requires "a sensitive and inherently discretionary judgment call" that the Constitution vests in the President "quite apart from any explicit congressional grant." *Dep't of the Navy v. Egan*, 484 U.S. 518, 527 (1988) (concluding that the MSPB lacked statutory authority to review the substance of an underlying decision to deny or revoke a security clearance); see also *id.* (The President's "authority to classify and control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to occupy a position in the Executive Branch that will give that person access to such information flows primarily from the [Commander-in-Chief Clause's] investment of power in the President."); *id.* ("The authority to protect [national security] information falls on the President as head of the Executive Branch and as Commander in Chief."). As the Supreme Court has concluded, "For 'reasons . . . too obvious to call for enlarged discussion,' *CIA v. Sims*, 471 U.S. 159, 170 (1985), the protection of classified information must be committed to the broad discretion of the agency responsible, and this must include broad discretion to determine

who may have access to it. Certainly, it is not reasonably possible for an outside nonexpert body to review the substance of such a judgment . . . .” *Egan*, 484 U.S. at 528.

## II. Other Concerns

### 1. Expanded Definition Of Protected Disclosure

Subparagraph 1(b)(1)(A) of the bill would broaden the definition of “protected disclosure” by amending 5 U.S.C. § 2302(b)(8)(A) to state:

any disclosure of information by an employee or applicant, *without restriction to time, place, form, motive, context, or prior disclosure made to any person by an employee or applicant, including a disclosure made in the ordinary course of an employee's duties* that the employee or applicant reasonably believes is evidence of

(i) *any violation* of any law, rule, or, regulation, or

(ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety. [emphasis added]

This amendment appears intended to override or supersede a series of decisions by the United States Court of Appeals for the Federal Circuit that defined the scope of disclosures covered by section 2302(b)(8). *See, e.g., Horton v. Dep't of Navy*, 66 F.3d 279, 282 (Fed. Cir. 1995) (complaints to wrongdoers are not protected whistleblowing); *Willis v. Dep't of Agriculture*, 141 F.3d 1139, 1143-44 (Fed. Cir. 1998) (ordinary work disagreements not protected disclosures, nor are disclosures made during the course of performing ordinary job duties); *Meuwissen v. Dep't of the Interior*, 234 F.3d 9, 12-14 (Fed. Cir. 2000) (discussion of matters already known does not constitute a covered disclosure); *LaChance v. White*, 174 F.3d 1378, 1381 (Fed. Cir. 1999) (in determining whether a disclosure is covered, the Board should consider the motives of the employee making the disclosure). The Federal Circuit precedent was useful to Federal agencies because it insulated them from having to defend against potentially burdensome whistleblower litigation involving no more than workplace disagreements, complaints by disgruntled employees, or matters that never were, in any real sense, “disclosed” to any individuals or organizations having any authority to address the disclosures.

The expanded definition in subparagraph 1(b)(1)(A) would upset the delicate balance between whistleblower protection and the ability of Federal managers to manage the workforce. The WPA already provides adequate protection for legitimate whistleblowers. The proposed expansive definition has the potential to convert any disagreement or contrary interpretation of a law, no matter how trivial or frivolous, into a whistleblower disclosure. It will not provide

further protection to those with legitimate claims, who are covered by the existing law. It simply will increase the number of frivolous claims of whistleblower reprisal. Such an increase in the number of frivolous claims would impose an unwarranted burden upon Federal managers and, ultimately, the MSPB and the Federal Judiciary.

The Federal Circuit appropriately has recognized that the purposes of the WPA must be taken into account in determining whether a disclosure is one protected by the WPA. *Willis v. Department of Agriculture*, 141 F.3d 1139, 1143 (Fed. Cir. 1998) (observing that “[t]he purpose of the WPA is to encourage government personnel to disclose government wrongdoing to persons who may be in a position to remedy the problem without fearing retaliatory action by their supervisors or those who might be harmed by the disclosures.”). Accordingly, the court in *Willis* recognized that expressing disagreement with a supervisor’s decision to that supervisor was not the type of disclosure protected by the WPA because it was not reporting the supervisor’s wrongdoing to anyone in a position to take action. *Id.* Moreover, the court found that the WPA was not intended to protect reports of violations of laws, rules, or regulations that an employee made as a part of his everyday job responsibilities. *Id.* at 1143-44.

These limitations are reasonable and serve to further the purpose of the WPA to protect legitimate whistleblowers. By prohibiting the consideration of “time, place, form, motive, context” and including the performance of one’s job duties in the definition of “disclosures,” the bill converts every Federal employee into a whistleblower. Nearly every Federal employee will, sometime during the course of his or her career, disagree with a statement or interpretation made by a supervisor, or during the course of performing his or her everyday responsibilities, report an error that may demonstrate a violation of a law, rule, or regulation. Without the ability to take the context – the time, the place, the motive – of the alleged disclosure into account, even trivial or *de minimis* matters would become elevated to the status of protected disclosures. *Cf. Herman v. Department of Justice*, 193 F.3d 1375, 1378-79 (Fed. Cir. 1999) (concluding that the WPA was not intended to apply to trivial matters). This provision would undermine the effectiveness of the WPA.

The danger of this expanded definition is even more apparent when understood in the context of the statutory scheme of the WPA. Under current law, once an individual has made a qualifying disclosure pursuant to 5 U.S.C. § 2302(b)(8), a *prima facie* case of whistleblower reprisal can be made by showing that a deciding agency official: a) knew of the disclosure; and b) an adverse action was taken within a reasonable time of the disclosure. *Kewley v. Department of Health & Human Serv.*, 153 F.3d 1357, 1362-62 (Fed. Cir. 1998) (citing 5 U.S.C. § 1221(e)(1)). Once the employee establishes this *prima facie* case, the burden shifts to the employing agency to show by clear and convincing evidence that it would have taken the adverse action regardless of the protected disclosure. *Kewley*, 153 F.3d at 1363.

Given the expanded definition of disclosure and the relatively light burden of establishing a *prima facie* case of reprisal under the knowledge/timing test, it would be exceedingly easy for



employees to use whistleblowing as a defense to every adverse personnel action. Then the statutory structure of the WPA would require the agency to meet the much higher burden of demonstrating by clear and convincing evidence that it would have taken the adverse action, regardless of the disclosure. Thus, for all practical purposes, section 1(b)(1)(A) would transform the statutory standard that an agency must meet in sustaining almost every adverse action from a preponderance of the evidence, 5 U.S.C. § 7701(c)(1)(B), to the clear and convincing standard required by 5 U.S.C. § 1221(e)(2).

The ease with which a Federal employee would be able to establish a *prima facie* case of whistleblower reprisal, no matter how frivolous, would seriously impair the ability of Federal managers to effectively and efficiently manage the workforce. If Federal managers knew that it was likely that they would be subject to a charge of whistleblower reprisal every time that they took an adverse personnel action, they might hesitate to take any such action. Likewise, the very low standards that would be required to advance a whistleblower claim would vastly increase the number of such claims, obscure the claims of legitimate whistleblowers, and unduly burden the MSPB and the Federal Circuit.

Currently, the WPA does not cover disclosures that specifically are prohibited by law or disclosures of information that specifically are required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs. Subparagraph 1(b)(3) would add 5 U.S.C. § 2302(b)(8)(C) to include this category of covered disclosures if the disclosure evidenced a reasonable belief of violation of law, rule, or regulation; gross mismanagement; gross waste of funds; abuse of authority; substantial and specific danger to public health or safety; *or* a false statement to Congress on an issue of material fact. The disclosure also would have to be made to a Member of Congress authorized to receive information of the type disclosed or to any employee of Congress having an appropriate security clearance and authorized to receive information of the type disclosed. The amendment would expand the scope of covered disclosures significantly and therefore substantially increase the potential exposure to litigation for Federal agencies as well as the staffing costs and other burdens associated with this issue.

## **2. Security Clearances**

There are three significant provisions regarding security clearances. First, subparagraph 1(e)(1) of the bill would amend 5 U.S.C. § 2302(a)(2)(A) to add “a suspension, revocation, or other determination relating to a security clearance,” to the definition of a personnel practice. Second, section 1(e)(2) (adding a new subparagraph (14) to 5 U.S.C. § 2302(b)) would amend the definition of prohibited personnel practices to include “conduct[ing] or caus[ing] to be conducted, an investigation, other than any ministerial or nondiscretionary fact finding activities necessary for the agency to perform its mission, of an employee or applicant for employment because of any activity protected under this section.” Third, subparagraph 1(e)(3) of the bill would authorize the MSPB and the courts to review these security clearance decisions to determine whether a violation of 5 U.S.C. § 2302 (prohibited personnel practices) had occurred

and, if so, to order certain relief. We have both general and technical objections to these provisions.

We strongly oppose these amendments because they would authorize the MSPB and the courts to review any determination relating to a security clearance – a prerogative left firmly within the Executive branch's discretion. See our constitutional objections, *supra*. This conflict is even more apparent in whistleblower cases. Under the WPA, a putative whistleblower establishes a *prima facie* case of whistleblower retaliation by establishing a protected disclosure and, under the knowledge/timing test, a personnel action taken within a certain period of time following the disclosure. Once the employee meets that minimal burden, the burden shifts to the agency to establish *by clear and convincing evidence* that it would have taken the action absent the protected disclosure.

Therefore, the bill would require in the security clearance context, that where individuals make protected disclosures (which, as we explain above, would include virtually every Federal employee under other amendments in this bill), the agency must justify its security clearance decision by the stringent standard of clear and convincing evidence. Thus, rather than awarding security clearances only where clearly consistent with the interests of national security, agencies would be permitted to deny or revoke them only upon the basis of clear and convincing evidence. This standard would be shockingly inconsistent with national security, especially in these times of heightened security concerns.

Beyond these objections, the amendments are simply unnecessary. Currently, Executive Order 12968 requires all agencies to establish an internal review board to consider appeals of security clearance revocations. These internal boards provide sufficient protections for the subjects of the revocations, while, at the same time, preserving the authority of the Executive branch to make the necessary decisions. In any event, we are not aware of any pattern of abusing security clearance decisions to retaliate against whistleblowers. Thus, the drastic and potentially unconstitutional amendments subparagraphs 1(e)(1) and 1(e)(3) would make are unwarranted.

We have other, more specific, objections to the bill. In defining the category of security clearance decisions that fall within a personnel action and, therefore, would be subject to review, subparagraph 1(e)(1) of the bill uses the phrase “suspension, revocation, or *any other determination* relating to a security clearance or any *other access determination by a covered agency*” [emphasis added]. Although the phrase “other determination” remains vague, the remainder of the provision, “or any other access determination by a covered agency,” is so broad as to encompass such things as an initial investigation into whether a security clearance is warranted, the decision to upgrade or downgrade a clearance, or any other decision connected in any way with a security clearance. This broad language would convert nearly every action an agency takes with regard to a security clearance into a possible basis for a whistleblower charge.

In addition, subparagraph 1(e)(2), amending the definition of prohibited personnel practices to include “conduct[ing] or caus[ing] to be conducted, an investigation, other than any ministerial or nondiscretionary fact finding activities necessary for the agency to perform its mission, of an employee or applicant for employment because of any activity protected under this section,” remains somewhat vague and potentially overly broad. Although this provision appears intended to allow the Government to conduct certain routine employment inquiries regarding current and prospective employees, it still will lead to disputes over the scope and permissibility of such inquiries.

Finally, subparagraph 1(e)(3) of the bill contains language stating that the MSPB or any reviewing court “may not order the President to restore a security clearance.” We presume this language was intended to alleviate concerns about the Executive branch prerogative with regard to security clearance determinations. However, the language, on its face, only prohibits the MSPB and reviewing court from ordering “the President” to “restore” a clearance. Conceivably, this language could be interpreted to allow the MSPB to order an agency head or lower official to restore the clearance. Likewise, it does not appear to limit the MSPB’s authority to order other actions with regard to security clearances, for instance, to award an initial clearance, to order an upgrade, or to stop an investigation. It also is unclear to us why a narrow class of whistleblower reprisal cases merits the “expedited review” subparagraph 1(e)(3) would require and what that would mean in this context.

### **3. Confidential Advice on Making Disclosures to Congress**

Subsection 1(m) would amend 5 U.S.C. § 2302(f) to require each agency to establish a procedure for providing confidential advice to employees on making lawful disclosures to Congress of information specifically required by law or Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs. This provision would place agencies in the odd and anomalous position of effectively encouraging their employees to disclose matters otherwise required by law to be kept secret. We oppose this provision.

### **4. Investigations**

Subparagraph 1(e)(1)(B) of the bill would amend 5 U.S.C. § 2302(a)(2)(A) to include within WPA-covered personnel actions “an investigation, other than any ministerial or nondiscretionary fact finding activities necessary for the agency to perform its mission, of an employee or applicant for employment because of any activity protected under this section.” Additionally, subparagraph 1(e)(2)(C) would amend 5 U.S.C. § 2302(b) to add new subparagraph (14), forbidding Federal employees to “conduct, or cause to be conducted, an investigation, other than any ministerial or nondiscretionary fact finding activities necessary for the agency to perform its mission, of an employee or applicant for employment because of any activity protected under this section.”

We are very troubled by the breadth of these provisions and the effect they could have on the ability of agencies to function. The amendments do not define adequately an "investigation." Accordingly, it would appear that any type of inquiry by any agency, ranging from criminal investigation to investigation for determining eligibility for a security clearance to Inspector General investigation to management inquiries of potential wrongdoing in the workplace, all could be subject to challenge and litigation.

Conceivably, any time a supervisor suspected wrongdoing by an employee and determined to look into the matter, the "investigation" could be subject to challenge. Certainly, any time an Office of Inspector General, an Office of Professional Responsibility, or similar agency component began an investigation, the investigation immediately could become the subject of litigation. Through such litigation, employees would be able to delay or thwart any investigation into their own or others' wrongdoing. This result could adversely affect the ability and perhaps even the willingness of supervisors to examine wrongdoing -- which clearly is not a beneficial outcome for the efficient and effective operation of agencies. Indeed, this provision could allow an employee to litigate an action that has not been proposed. Thus, even before any discipline had been proposed or any charges brought, the employee could attempt to short circuit any inquiry into the situation. In this connection, we note that the Equal Employment Opportunity Commission has prohibited the filing of a formal complaint on a "proposal to take a personnel action, or other preliminary step to taking a personnel action." *See* 29 C.F.R. § 1614.107(a)(5).

The CSRA is a careful balance between providing remedies for personnel actions that have been taken against Federal employees and permitting agencies to manage their workforces effectively. Subparagraphs 1(e)(1)(B) and 1(e)(2)(C) would upset that balance seriously, since an investigation is not an action against the employee but is a necessary government function for gathering facts about a wide range of matters so that informed decisions can be subsequently made.

Further, including conducting investigations and "causing them to be conducted" among the prohibited practices could decrease the willingness of any employee to report allegations of misconduct to an Office of Inspector General ("OIG"), which is generally responsible for conducting such investigations. Even the reporting of wrongdoing could be viewed as causing an investigation to be conducted and could subject not just investigators and managers but any employee who "causes" an investigation to be conducted to charges of committing a prohibited personnel practice.

Moreover, the allegation of a prohibited personnel practice in the form of an investigation could result in an investigation by the Office of Special Counsel into an open criminal or administrative investigation and into open investigatory files, and then, pursuant to the OSC's statutory obligations, the reporting of that investigatory information to the complainant. Except in limited circumstances, open investigative files are not shared with other agencies or persons

for several reasons, including the privacy interests of the subject and witnesses, and the protection of investigative techniques. Additionally, the Inspector General Act of 1978, as amended, 5 U.S.C. app. § 7(a), requires that the confidentiality of a Federal employee complainant be maintained “unless disclosure is unavoidable during the course of an investigation.” Our concerns are amplified because of OSC's reporting of the progress of its investigation and its findings to the complainant. This reporting could compromise and undermine a legitimate law enforcement investigation.

## **5. Attorneys Fees**

Subsection 1(g) of the bill would amend 5 U.S.C. § 1204(m)(1) to provide that, in disciplinary action cases, a prevailing employee could obtain attorneys fees from the agency at which the prevailing party was employed rather than, as currently exists, from the agency proposing the disciplinary action against the employee. Essentially, this provision would shift the burden for attorneys fees from the Office of Special Counsel, the agency responsible for pursuing disciplinary actions, to the prevailing party's employing agency. We object to this change for at least two reasons. First, one of the general policies underlying fee-shifting provisions against the Government is ensuring that the Government acts responsibly. By shifting the burden from the agency responsible for taking disciplinary actions – the Special Counsel – to the employing agency, this amendment would eliminate this important check on the Special Counsel in considering which actions to pursue because even if the Special Counsel took an unjustified action, it will not have to bear the attorneys fees. Second, this amendment is patently unfair to the employing agencies, which might disagree with the action the Special Counsel was pursuing but nevertheless would be responsible for any fees. Indeed, it is not uncommon that an agency will refuse to take a disciplinary action that is proposed by the Special Counsel, agreeing with a particular employee that no wrongdoing had been committed. If the employee hired an attorney and successfully defended himself against the Special Counsel before the MSPB or the Federal Circuit, the employing agency – who disagreed with the Special Counsel's actions – would be required to pay the fees.

Finally, we recognize that under 5 U.S.C. § 2302(a)(2)(C)(ii), certain intelligence agencies are exempt from the Whistleblower Protection Act. However, subsection 1(f) of the bill would amend that provision, so that other agencies responsible for handling classified information on a regular basis (such as the Departments of Homeland Security, Justice, State, and Defense) would not be exempt, unless the President specifically designated them as exempt prior to any personnel action alleged to be in reprisal for whistleblowing.

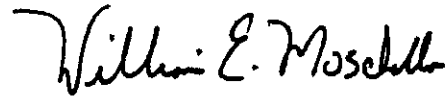
Thank you for the opportunity to present our views. Please do not hesitate to call upon us if we may be of additional assistance. The Office of Management and Budget has advised us that

The Honorable Susan M. Collins

Page 13

from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,

A handwritten signature in black ink, reading "William E. Moschella". The signature is written in a cursive style with a large, stylized "W" and "M".

William E. Moschella  
Assistant Attorney General

cc: The Honorable Joseph I. Lieberman  
Ranking Minority Member



U.S. Department of Justice

Office of Legislative Affairs

---

Office of the Assistant Attorney General

Washington, D.C. 20530

June 15, 2005

The Honorable Daniel K. Akaka  
Ranking Minority Member  
Subcommittee on Oversight of Government Management,  
the Federal Workforce, and the District of Columbia  
Committee on Homeland Security and Governmental Affairs  
United States Senate  
Washington, D.C. 20510

Dear Senator Akaka:

This letter responds to your letter of October 20, 2004, regarding the Department of Justice views letter of October 8, 2004, to Chairman Collins concerning S. 2628 from the prior Congress, the "Federal Employee Protection of Disclosures Act," pending in the current Congress as S. 494. We appreciate learning of your concerns and hope this response will address them.

**Constitutional Concerns**

We have reviewed your analysis of the provisions in the bill that we consider unconstitutional. We remain unable to reconcile those provisions with the Constitution. Our understanding represents the longstanding view of the Executive branch and is consistent with judicial precedent.

In particular, we continue to strongly oppose subparagraph 1(b)(3) as unconstitutional. This provision would permit any covered Executive branch employee or applicant to disclose to Congress classified national security information without receiving official authorization to do so. Indeed, you describe this subsection as clarifying that Executive branch employees have a "right" to furnish national security information to Congress without official authorization. It would unconstitutionally deprive the President of his authority to decide, based upon the national interest, how, when, and under what circumstances particular classified information should be disclosed to Congress.

Not only does the Constitution generally establish the President as the head of the Executive branch, it also makes him Commander in Chief of all military forces, the sole organ of America's foreign affairs, and the officer in the Government with the express duty (and

corresponding authority) to take care that the laws are faithfully executed. The President's authority to classify and control access to national security information in the Executive branch flows directly from these powers, as both this Department and the courts long have recognized. *See Dep't of the Navy v. Egan*, 484 U.S. 518, 527 (1988); *see also New York Times Co. v. United States*, 403 U.S. 713, 729-30 (1971) (Stewart, J., concurring) ("[I]t is clear to me that it is the constitutional duty of the Executive — as a matter of sovereign prerogative and not as a matter of law as the courts know law — through the promulgation and enforcement of executive regulations, to protect the confidentiality necessary to carry out its responsibilities in the fields of international relations and national defense."); *Common Legislative Encroachments on Executive Branch Authority*, 13 Op. O.L.C. 248, 254 (1989) (describing "the President's constitutional responsibility to protect certain information"). The recognition of this authority stretches back to the earliest days of the Republic and across many partisan divides. *See History of Refusals by Executive Branch Officials to Provide Information Demanded by Congress*, 6 Op. O.L.C. 751 (1982) (compiling historical examples of cases in which the President withheld from Congress information the release of which he determined could jeopardize national security); *Congressional Requests for Confidential Executive Branch Information*, 13 Op. O.L.C. 153, 154 (1989) (stating that the privilege "has been asserted by numerous Presidents from the earliest days of our nation").

Your letter questions our reliance on *Egan*, contending that it "is fundamentally a case of statutory construction." Although the ultimate question in that case was statutory, in interpreting the statute in question, the Supreme Court expressly recognized the constitutional foundation of the President's authority to protect national security information:

The President, after all, is the "Commander in Chief of the Army and Navy of the United States." U.S. Const., art. II, § 2. His authority to classify and control access to information bearing on national security . . . flows primarily from this constitutional investment of power in the President and exists quite apart from any explicit congressional grant. . . . The authority to protect such information falls on the President as head of the Executive Branch and as Commander in Chief.

*Egan*, 484 U.S. at 527; *see also, e.g., Hill v. Dep't of the Air Force*, 844 F.2d 1407, 1410 (10th Cir. 1988) (acknowledging that the President's authority to protect national security information is constitutionally based). You also quote language from *Egan* stating that, "unless Congress specifically has provided otherwise, courts traditionally have been reluctant to intrude upon the authority of the Executive in military and national security affairs." However, read in context, this language merely confirms that in the areas of foreign policy and national security, courts have shown deference to both elected Branches. *See Egan*, 484 U.S. at 530. Indeed, each of the five cases that the Court cites following the language you quote supports judicial deference to both the President and Congress. This is a proposition much different from that urged in your letter. It hardly follows from this tradition of judicial deference to the political Branches that the Court is obliquely suggesting a power of Congress to usurp the President's longstanding power



over national security information. Not one of these cases addresses — much less supports — such congressional intrusion. *Egan* explicitly recognized the “constitutional investment of power in the President,” which “exists quite apart from any explicit congressional grant,” “to classify and control access to information bearing on national security.” *Id.* at 527. That the “Constitution nowhere expressly states that the President, or the executive branch generally, enjoys a privilege against disclosing information requested by . . . the legislative branch” does not diminish this authority, which “is a necessary corollary of the executive function vested in the President by Article II of the Constitution.” 13 Op. O.L.C. at 154; *see also United States v. Nixon*, 418 U.S. 683, 706-07 n.16, 711 (1974) (specifically holding that executive privilege is constitutionally based even though not expressly provided for in the Constitution).

Of course, the Department agrees that Congress has an interest in receiving the information that enables it to carry out its important oversight responsibilities. In fact, we long have recognized this interest, even while safeguarding the interests of the Executive branch. *See, e.g.*, 13 Op. O.L.C. at 153-54. However, subparagraph 1(b)(3) is unnecessary to satisfy this interest. The Executive branch remains committed to accommodating Congress’s legitimate oversight needs in ways that are consistent with the Executive branch’s constitutional responsibilities. A process exists by which this has been and may be done. *See* 13 Op. O.L.C. at 157-61. As we have explained, “[t]he process of accommodation requires that each branch explain to the other why it believes its needs to be legitimate. . . . If either branch has a reason for needing to obtain or withhold information, it should be able to express it.” *Id.* at 159. Subsection 1(b)(3) would circumvent this longstanding process unilaterally, by allowing any covered employee with access to classified information to go directly to Congress. The process of dynamic compromise between the Branches, whereby each Branch seeks an optimal accommodation by evaluating the needs of the other, cannot function where every covered employee of the Executive branch is vested with the right to determine for himself or herself, without any official authorization, those disclosures that are appropriate.

For similar reasons, we continue to object to subparagraph 1(e)(2), subsection 1(k), and subparagraph 1(e)(3) of the bill and recommend that these provisions be deleted. Subparagraph 1(e)(2) and subsection 1(k) purport to dictate and micromanage the specific content of nondisclosure agreements applicable to Executive branch employees and contractors. Subparagraph 1(e)(3) purports to require the Merit Systems Protection Board (“MSPB”) or any reviewing court, in any security clearance appeal, to review and decide whether a security clearance determination was made because the employee disclosed information — including national security information — that the bill permits the employee to disclose. These provisions purport to divest the President of his control over national security information in the Executive branch and thereby impermissibly intrude upon the President’s constitutional authority to classify and control access to national security information.

### Other Concerns

In our prior letters and testimony, we have addressed many of the points raised by your letter. We do not believe it appropriate to reiterate this information in its entirety here. However, we would like to make several additional points.

As to your first point, that the Department said that agencies “can discipline employees for whistleblowing,” our statement may have been somewhat imprecise and unduly provocative. Nevertheless, the reality is — as Congress has recognized in exempting certain agencies from procedural protections for prohibited personnel practices (including retaliation for whistleblowing) — some employees, by virtue of their sensitive duties in the intelligence community and routine access to national security information, simply are not and should not be as free to disclose information about their work as are other employees. That is, an employee in such a position should not expect protection if he or she improperly discloses information about the work of his or her intelligence agency. Indeed, improper disclosure of sensitive information not only can subject employees to discipline; it can be a criminal offense.<sup>1</sup> If these disclosures were protected, then protection of national security information would be jeopardized. Thus, while such employees may have some protections for limited disclosures in certain controlled contexts, the full panoply of whistleblower protections that applies to many Federal employees does not apply to employees in some agencies.

Thus, this shorthand reference should not be taken as bias against whistleblowers, but merely a recognition that a different balance of protection has been and should be struck as to some employees in particularly sensitive agencies. On the contrary, the Department is committed to protecting whistleblowers and toward that end, it has promulgated regulations<sup>2</sup> to afford the carefully crafted protections for FBI whistleblowers contemplated in 5 U.S.C. § 2303.

---

<sup>1</sup>See, e.g., 18 U.S.C. § 793, making it a crime to disclose information relating to the national defense to persons not authorized to receive it. This statute covers most, but not all, unauthorized disclosures of classified information. In addition, 18 U.S.C. § 798 makes it a crime to disclose to unauthorized persons classified information concerning cryptographic systems and the communications intelligence activities of the United States.

<sup>2</sup>28 C.F.R. Part 27 creates a system for protecting FBI whistleblowers that is similar to the system applicable to other Federal employees. These regulations give the Department’s inspector general and its Office of Professional Responsibility an investigatory and prosecutorial role similar to that of the Office of Special Counsel. They give the Office of Attorney Recruitment and Management an adjudicatory role similar to that of the Merit Systems Protection Board.

## 1. Authority of the Special Counsel

In your letter, you compare the litigating authority the bill would grant to the Office of Special Counsel ("Special Counsel") to that currently granted to the chief counsel of the Small Business Administration ("SBA"). We believe that these authorities would operate quite differently. First, unlike the SBA, the Special Counsel deals with issues affecting numerous Executive branch agencies. It is imperative that the Executive branch speak with one voice as to those issues in court.

Furthermore, as we said in response to questions arising from the November 12, 2003, hearing before the Senate Committee on Governmental Affairs concerning S. 1358 (the "Federal Employee Protection of Disclosures Act"), the litigation authority given the Federal Labor Relations Authority ("FLRA") differs from that proposed for the Special Counsel, because, unlike the Special Counsel, the FLRA is a quasi-judicial entity defending its decisions in court. And as we stated in that response, "[i]n our experience with the [Special Counsel], we believe the Department has capably represented the [Special Counsel] before the Federal Circuit and we have not had any feedback from the [Special Counsel] to indicate otherwise." "Moreover, as a general policy, it is undesirable to increase the number of situations in which Executive branch agencies could litigate against each other" or take different positions in the same case, such as through the provision of amicus briefs.

## 2. Confidential Disclosures to Congress

We believe that the discussion in your letter of confidential disclosures to Congress under 5 U.S.C. § 2302(b) is imprecise. The end of 5 U.S.C. § 2302(b) simply states that "[t]his subsection shall not be construed to authorize the withholding of information from the Congress or the taking of any personnel action against an employee who discloses information to the Congress." While subsection 2302(b) shall not be construed to "authorize" a personnel action against an employee who discloses information to Congress, the statute does not provide protection for an employee who does so, to the extent that the disclosure is specifically prohibited by law or "required by Executive Order to be kept secret in the interest of national defense or the conduct of foreign affairs." 5 U.S.C. § 2302(b)(8)(B). As to such information, the statute provides that employees are protected only if they disclose the information to an inspector general or to the Special Counsel. This scheme adequately and properly strikes a balance between the Executive branch's responsibilities for the protection of classified information and the protection of whistleblowers.

We previously set forth our views on *Egan* and the appropriate procedure for the Executive branch to disclose classified information to the Legislative branch.

### 3. Protected Disclosures and Presumption of Government Good Conduct

The discussion in your letter relating to the scope of protected disclosures does not address the Department's point that vastly expanding the definition of protected disclosure to include the phrase "without restriction to time, place, form, motive, context or prior disclosure to any person by an employee or applicant, including a disclosure made in the ordinary course of an employee's duties" will convert every Federal employee into a whistleblower, because nearly every employee at some point has at least a minor disagreement with their supervisor, or will report an error in the course of his or her everyday duties, that may demonstrate a violation of law, rule or regulation. It is not enough to argue, as your letter does, that the Office of Special Counsel ("OSC") can weed out frivolous claims, because even where the OSC may reject a whistleblower claim, the employee can nonetheless proceed to the Merit Systems Protection Board for a de novo review, and then to the Court of Appeals Federal Circuit, thereby unduly burdening those panels as well. Moreover, as our October 8, 2004, letter explained, the prima facie burden that the employee must prove can be based on mere circumstantial evidence, and then the agency must prove by the heavy burden of clear and convincing evidence that it would have taken the personnel action at issue in any event. Thus, the agency's burden of sustaining almost all actions for poor performance or misconduct is greatly increased beyond the substantial evidence and preponderance of evidence standards that would otherwise apply. This scheme would clearly upset the delicate balance between whistleblower protection and the ability of Federal supervisors to manage the workforce.

### 4. Security Clearances

We believe that the reference to *Hess v. State*, 217 F.3d 1372 (Fed. Cir. 2000), in your discussion of revoking security clearance is inapt. In *Hess*, the Federal Circuit followed longstanding Supreme Court precedent, *i.e.*, *Egan*, in finding that the MSPB did not have jurisdiction to review security clearance determinations. Thus, *Hess* does not suggest the need for statutory change. Indeed, the same considerations recognized by the Court in *Egan* apply with equal force to any MSPB review of security clearance determinations because of allegations of retaliation for whistleblowing.

Additionally, the bill's proposed relaxation in the standard for revoking clearances, from the clear and convincing evidence standard to the preponderance of the evidence standard, would not alleviate our concerns. The bottom line remains that rather than applying the appropriate standard that all doubt is resolved in favor of national security, the preponderance of evidence standard would require that the benefit of the doubt be given to granting access to classified information, rather than protecting national security.

5. Education Provisions

The bill would require agencies to set up procedures for advising their employees on how to make disclosures of classified information to Congress. Your letter states your concern about our objection to this provision. However, we believe our concerns that Federal agencies not encourage their employees to disclose national security information that is required to be kept secret are legitimate. We continue to oppose this provision.

6. Retaliatory Investigations

In our letter of October 8, 2004, we stated our concern that litigation over whether an investigation was retaliatory could have a significantly chilling effect upon investigations by an inspector general, by our Office of Professional Responsibility, or by a similar agency or office. We do not agree that excluding undefined "ministerial or nondiscretionary fact finding activities" would address this concern fully. Even if, as your letter posits, this phrase would include criminal investigations, the provision would open an array of potential litigation and seriously compromise the ability of agencies to make necessary administrative inquiries into possible wrongdoing.

7. Attorney Fees

Your letter states that requiring agencies to pay the attorney fees of managers wrongly disciplined by the Special Counsel would operate as a check on those agencies against retaliation, consistent with the No FEAR Act. However, we continue to believe that shifting the fee burden from the Special Counsel to the employing agency would undermine both the values of accountability, *i.e.*, requiring the Special Counsel to internalize the consequences of not exercising its discretion properly, and fairness, *i.e.*, not holding an employing agency responsible for disciplinary action in which it may have had no part.

Thank you for your consideration of our views. Please do not hesitate to call upon us if we may be of further assistance in this matter. The Office of Management and Budget has advised us that from the standpoint of the Administration's program, there is no objection to submission of this letter.

Sincerely,

A handwritten signature in black ink, reading "William E. Moschella". The signature is fluid and cursive, with the first name "William" and last name "Moschella" clearly legible.

William E. Moschella  
Assistant Attorney General

The Honorable Daniel K. Akaka

Page 8

cc: The Honorable George V. Voinovich  
Chairman  
Subcommittee on Oversight of Government Management,  
the Federal Workforce, and the District of Columbia  
Committee on Homeland Security and Governmental Affairs

The Honorable Susan M. Collins  
Chairman  
Committee on Homeland Security and Governmental Affairs

The Honorable Joseph I. Lieberman  
Ranking Minority Member  
Committee on Homeland Security and Governmental Affairs



Office of the Attorney General  
Washington, D. C. 20530  
August 29, 2005

The Honorable Arlen Specter  
Chairman  
Committee on the Judiciary  
United States Senate  
Washington, D.C. 20510

The Honorable Pat Roberts  
Chairman  
Select Committee on Intelligence  
United States Senate  
Washington, D.C. 20510

The Honorable F. James Sensenbrenner, Jr.  
Chairman  
Committee on the Judiciary  
U. S. House of Representatives  
Washington, D.C. 20515

The Honorable Peter Hoekstra  
Chairman  
Permanent Select Committee on Intelligence  
U.S. House of Representatives  
Washington, D.C. 20515

Dear Messrs. Chairmen:

We understand that conferees will soon consider the House and Senate versions of H.R. 3199, the "USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005." We write to provide the Conference with the Administration's views on these important bills.

The President has called on Congress to renew all parts of the USA PATRIOT Act ("the Act") that are scheduled to sunset. As the President has repeatedly cautioned, the terrorist threat against this country will not sunset, and neither should the tools we use to combat terrorism. The USA PATRIOT Act has been, and should continue to be, an essential tool in the effort to combat terrorism and protect the American people. The Act has increased our ability to share intelligence information, updated the law to address changes in technology, and provided the FBI critical tools to investigate terrorists and spies that have been used for years to investigate organized crime and drug dealers. We share your commitment to the protection of civil liberties and are pleased that there have been no verified abuses of the Act. *See, e.g.,* U.S. Department of Justice Office of the Inspector General: Report to Congress on Implementation of Section 1001 of the USA PATRIOT Act (August 15, 2005).

The Department of Justice has carefully reviewed the House and Senate versions of H.R. 3199. These bills contain many provisions that the Administration supports. For example, we appreciate the permanent reauthorization of 14 of the 16 sunseting USA PATRIOT Act provisions. The House version of H.R. 3199 also includes many important and potentially valuable provisions that do not directly amend USA PATRIOT Act provisions. Our support for such provisions is explained in detail in the enclosure to this letter. However, in our judgment both bills also contain provisions that weaken some of the most important and useful authorities in the Act. We are particularly concerned about proposed amendments to sections 206 and 215 of the Act. These concerns are discussed in more detail below and in the enclosure.

Under section 206 of the USA PATRIOT Act, the Foreign Intelligence Surveillance Court ("FISA Court") may authorize investigators to surveil each communications device that a target uses, even if the target switches telecommunications providers, if the target's actions "may have the effect of thwarting the identification of a specified person" (18 U.S.C. § 1805(2)(B)). This is sometimes referred to as "multi-point" or "roving" surveillance, and it can be essential in effectively tracking a terrorist or spy trained to avoid detection. We are concerned that the Senate bill's amendments to the standard for issuing a section 206 order would make this critical investigative tool – a tool available in the criminal context for many years – more difficult to use. We therefore urge the Senate to recede to the House bill's provision concerning section 206.

Section 215 of the USA PATRIOT Act amended the Foreign Intelligence Surveillance Act of 1978 ("FISA") to allow the FISA Court to order production in foreign intelligence investigations of the same kinds of materials that prosecutors always have been able to obtain through grand jury subpoenas. Because of concerns with the Senate bill's amendments to section 215, we strongly encourage the Senate to recede to the House bill's amendments to that provision. For example, we are concerned that the Senate's amendment of the section 215 standard could be construed to increase the Government's burden in obtaining a section 215 order substantially and thereby limit the use of this important counterterrorism tool. Moreover, the Senate would allow the FISA Court to order disclosure of portions of the court's order and related materials, potentially putting highly sensitive, classified national security information at risk. We prefer the House bill's procedure for judicial review of a section 215 order, and we urge the Senate to recede to the House version on this point as well.

Finally, we are also concerned about a number of other provisions, including amendments to the critical information sharing provisions of USA PATRIOT Act section 203(b), amendments to the National Security Letter statutes, increased reporting requirements, and new sunset provisions. These additional concerns and several suggested technical improvements are described in detail in the enclosure to this letter.



The Honorable Arlen Specter, Pat Roberts, F. James Sensenbrenner, Jr., and Peter Hoekstra  
Page 3

We appreciate the hard work that Congress has undertaken in examining the USA PATRIOT Act, and we thank Congress for the opportunity to present our views. We look forward to the opportunity to work with the Conference further on these important issues. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to submission of this letter.

Sincerely,



Alberto R. Gonzales  
Attorney General

Enclosure

cc: The Honorable Patrick J. Leahy  
Ranking Minority Member  
Committee on the Judiciary  
United States Senate

The Honorable John D. Rockefeller IV  
Vice Chair  
Select Committee on Intelligence  
United States Senate

The Honorable John Conyers, Jr.  
Ranking Minority Member  
Committee on the Judiciary  
U.S. House of Representatives

The Honorable Jane Harman  
Ranking Minority Member  
Permanent Select Committee on Intelligence  
U.S. House of Representatives

## ENCLOSURE

### USA PATRIOT Act Provisions: Senate version; House version, Title I

#### USA PATRIOT Act Section 203(b)

**House version, section 105. Sharing of Electronic, Wire, and Oral Interception Information Under Section 203(b) of the USA PATRIOT Act.** It is now widely accepted that a lack of information sharing and coordination within our government prior to the attacks of September 11, 2001, compromised this Nation's ability to "connect the dots" and prevent terrorist attacks. *See, e.g.,* The Report of the Joint Inquiry Into the Terrorist Attacks of September 11, 2001; The National Commission on Terrorist Attacks Upon the United States (9-11 Commission) Report (collectively the "September 11 Reports"). This failure was attributable in part to legal restrictions on the disclosure of information.

Section 203(b) of the USA PATRIOT Act, codified at 18 U.S.C. § 2517(6), was one of several provisions in the Act that facilitated information sharing and helped to close the dangerous gap between law enforcement officials and members of the intelligence and national security communities. This section allowed law enforcement to disclose the contents of any court-ordered Title III wiretap, or evidence derived therefrom, to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence information to assist the official in the performance of his official duties. Disclosures under section 203(b) have been used, among other things, to track terrorists' funding sources and to identify terrorist operatives overseas.

Section 203(b) did not eliminate any of the important safeguards that exist with respect to a wiretap order, and additional safeguards must be in place before any disclosure under section 203(b) may be made. In order to obtain a wiretap, law enforcement must: (1) apply for and receive a court order; (2) establish probable cause that a particular offense has been or is about to be committed; (3) establish probable cause that communications concerning that offense will be obtained through the wiretap; and (4) provide an explanation to the court as to attempts to use other investigative procedures. Not only are wiretaps subject to prior court approval, but Title III provides for ongoing court supervision and reporting provisions.

The information sharing permitted under section 203(b) is limited. First, section 203(b) only allows for the sharing of a certain limited class of information gathered under Title III, such as information related to serious national security matters. It does not provide authority to share all information gathered under Title III authority. In addition, an individual who receives any information from a criminal investigative wiretap may use it "only as necessary in the conduct of that person's official duties [and] subject to any limitations on the unauthorized disclosure of such information." 18 U.S.C. § 2517(6). Moreover, the Attorney General has issued binding privacy guidelines governing the sharing of information that identifies a United States person. These guidelines require that all of such information be labeled before disclosure and handled according to specific protocols designed to ensure its appropriate and limited use.

The Department believes that section 105 of the House version of H.R. 3199 would severely hamper information sharing by requiring the Federal government to file a notice with the judge who originally authorized the Title III wiretap each time a disclosure of the contents of an intercepted communication was made pursuant to section 203(b). Under section 105, the required notice would both state that contents were disclosed and indicate the departments, agencies, or entities to which the disclosure was made. We are concerned that the requirements of section 105 would prevent information from being shared in a timely manner, if at all. The September 11 Reports found that requirements similar to this notice requirement result in a culture of risk aversion; in other words, when faced with the notice requirement found in section 105, government officials might revert to an unduly conservative approach to the sharing of vital information with other law enforcement agencies, out of fear of violating the notice law and subjecting themselves to all the civil and administrative sanctions that result from Title III violations and potentially subjecting vital evidence to suppression. At the very least, delays would occur while officials sought guidance on the notice requirement's applicability and determined whether information at issue contained contents of an intercepted communication. A culture could very well develop in which information that could be shared in compliance with the provisions of the statute would nonetheless not be shared because of bureaucratic barriers. This would undermine the central purpose of the information-sharing provisions in the USA PATRIOT Act was to eliminate legal and cultural barriers to the information sharing that has become critical to our counter-terrorism efforts. Congress should not enact a notice provision that has the potential to reimpose those barriers.

The problem is compounded because section 105 contains no time limit, so even if a disclosure is made years after the conclusion of a wiretap, section 105 would still require notice to the court that authorized the wiretap. By contrast, judicial supervision of the wiretap itself is generally limited to the time period during which communications are being intercepted. One can imagine the burden that would arise in tracking disclosures and fulfilling notice requirements years after a wiretap has ended. Another concern is that this notice requirement could put sensitive information at risk. Although notice is given to the court under seal, which offers some protection, there is no prohibition or limitation on sharing the contents of the notice filing, thus possibly providing a roadmap to the Government's information-sharing efforts, on a disclosure-by-disclosure basis. These notices would not only indicate that investigators thought that communications included foreign intelligence information, but detailing the precise agencies to which the information was disclosed could also provide insight into our national security efforts. For these reasons, the Department is deeply concerned about the effects of section 105, and we cannot support it. We urge the House to recede to the Senate's position on this important issue.

#### **USA PATRIOT Act Section 206**

**Senate version, section 2. USA PATRIOT Act Section 206; Additional Requirements for Multipoint Electronic Surveillance Under FISA (Amending Section 206 of USA PATRIOT); House version, section 109. Specificity and Notification for Roving Surveillance Authority Under Section 206 of the USA PATRIOT Act.** Where the actions of a target of FISA surveillance "may have the effect of thwarting the identification of a specified person," 18 U.S.C. § 1805(2)(B), section 206 of the USA PATRIOT Act enables the FISA Court to issue an order allowing investigators to surveil each communications device that the target

uses, even if the target switches telecommunications providers (referred to as “multi-point” or “roving” surveillance). A similar authority has been available in criminal investigations since 1986. As of March 30, 2005, the FISA Court had issued orders under section 206 of the USA PATRIOT Act 49 times. It has been effective in investigating international terrorists and spies, who are often trained to take sophisticated measures to evade detection.<sup>1</sup> Both the House and the Senate have passed substantive modifications to FISA electronic surveillance authority. In addition, both would subject section 206 of the USA PATRIOT Act to an additional sunset.

Under current law, the FISA Court’s electronic surveillance order must identify the target, if known, or otherwise describe the target with sufficient detail to distinguish that target from other persons. The ability to provide the court with a description of the target and not the target’s identity is crucial when the Government knows a good deal about a target but does not know the target’s actual name because, for example, the target is a spy trained to conceal it. Moreover, to authorize surveillance (multi-point or not), the FISA Court must find probable cause that the target is a foreign power or an agent of a foreign power. Thus, in all cases, the Department is required to present a sufficiently detailed description to allow the FISA Court to determine that the target is a foreign power or an agent of a foreign power, even if the target cannot be identified by name.

Section 2 of the Senate version would amend FISA to require that a FISA Court surveillance order “include sufficient information to describe a *specific target with particularity*” if the identity of the target is not known. (Emphasis added.) Section 2 would thus raise the current standard in two ways—adding “specific” before “target” and “with particularity” after “target.” There is a very real concern that the FISA Court would construe this doubly amended standard to increase substantially the required specificity in describing the target. *See Wallace v. Jaffree*, 472 U.S. 38, 59 n.48 (1985) (there is a “common-sense presumption that statutes are usually enacted to change existing law”). Hence, section 2 would likely make it more difficult for the Government to obtain these critical wiretaps in national security investigations, and we therefore cannot support it.

We urge the Senate to recede to the House on this provision. Section 109 of the House version also seeks to raise the standard for obtaining section 206 wiretaps, requiring the Court to make a finding, “based on specific facts provided in the application,” that the actions of the target might have the effect of thwarting surveillance. Although the House bill would impose an additional requirement before a section 206 wiretap could be obtained, we believe it would be less likely to prevent national security investigators from using this important tool. We also offer the following suggestion to the conferees: inserting the word “specific” before “target” would satisfy the desire to ensure adequate specificity where the identity of the target is not known, without raising the same concern that the Senate bill currently does—namely, that it arguably heightens the standard twice.

Both the House and Senate would also impose a so-called “return” requirement, intended to require the Government to provide notice to the FISA Court after “going up” on a new facility. We view such a requirement as unnecessary given the safeguards already in place with respect to

---

<sup>1</sup> A more specific discussion of section 206 has been provided to both the House and the Senate in classified form. We have attached a declassified letter here, redacted to protect national security, for the conferees’ convenience.

FISA surveillance, and we do not support imposing such a requirement. In the event that a return requirement is adopted, we urge the House to recede to the Senate on this issue; owing to differences in language, the House version would be significantly more burdensome without providing any additional meaningful oversight. We further urge the conferees to allow investigators to return to court within a reasonable time, as opposed to the inflexible 10-day limit currently in the Senate version. Making such a modification would allow the FISA Court to assess the circumstances of a particular case in determining when it is appropriate to file a return.

### **USA PATRIOT Act Section 207**

**Senate version, section 3. USA PATRIOT Act Section 207; Duration of FISA Surveillance of Non-United States Persons; House version, section 106. Duration of FISA Surveillance of Non-United States Persons Under Section 207 of the USA PATRIOT Act.** Section 207 of the USA PATRIOT Act increased the maximum time duration for certain surveillance and physical search orders issued by the FISA Court. The shorter timeframes that existed prior to the USA PATRIOT Act forced Government attorneys and agents needlessly to divert manpower away from the primary mission of detecting and disrupting potential terrorist attacks in order to return frequently to the FISA Court to ask for routine extensions of FISA orders. As the Attorney General testified before the Senate Judiciary Committee, the Department estimates that the extended durations authorized by section 207 saved the Department at least 60,000 hours of attorney time.

Both the House and the Senate versions would again increase the maximum available duration of certain FISA Court orders—a proposal that was supported by the recent report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (“WMD Commission”). If adopted, we conservatively estimate that these amendments would save the Department thousands of attorney hours per year, a figure that does not include the time that would be saved by agents and attorneys at the FBI and administrative staff within the Department. We therefore strongly support the extended durations included in both the House and Senate bills.

### **USA PATRIOT Act Section 212**

**Senate version, section 4. USA PATRIOT Act Section 212; Enhanced Oversight of Good-Faith Emergency Disclosures; House version, section 108. Report on Emergency Disclosures Under Section 212 of the USA PATRIOT Act.** Before the USA PATRIOT Act, computer-service providers could not disclose customer communications and records in emergency situations without fear of liability. If an Internet Service Provider (ISP) notified law enforcement that a customer was about to commit a terrorist attack, the ISP might be subject to civil lawsuits.

Section 212 of the USA PATRIOT Act allows computer-service providers to disclose voluntarily both the content of a communication and customer records in life-threatening emergencies without fear of civil liability. Providers are permitted—but not required—to disclose information to a governmental entity if the provider, in good faith, believes that an emergency involving imminent danger of death or serious physical injury to any person requires

disclosure of communications. Codified at 18 U.S.C. § 2702(b)(8) and 2702(c)(4), section 212 imposes no obligation on providers to review customer communications in search of such imminent dangers. Nor are ISPs compelled to provide anything to the Government, even if the Government approaches them with respect to this authority.

Communications providers have used this authority to disclose vital information in a number of important investigations. Section 212 disclosures assisted law enforcement in locating an 88-year-old woman who had been kidnapped and was being held in an unheated shack during a Wisconsin winter, in recovering a 13-year-old girl who had been lured and held captive by a man she met online, and in multiple investigations of credible threats of attacks directed against mosques. Section 212 disclosures have also played a vital role in suicide prevention by allowing ISPs to inform law enforcement of such threats.

There have been no reported or verified abuses of this provision. We therefore view as needlessly burdensome the new reporting requirement found in both the House and the Senate versions.

### **USA PATRIOT Act Section 213**

**Senate version, section 5. USA PATRIOT Act Section 213; Limitations on Delayed Notice Search Warrants; House version, section 114. Definition of Period of Reasonable Delay Under Section 213 of the USA PATRIOT Act.** Delayed-notice search warrants have been available for decades and were in use long before the USA PATRIOT Act was enacted. Section 213 of the USA PATRIOT Act merely created a nationally uniform process and standard for obtaining them. Like all criminal search warrants, a delayed-notice search warrant is issued by a Federal judge only upon a showing that there is probable cause to believe that a crime has been or will be committed and that the property sought or seized constitutes evidence of such criminal offense. A delayed-notice warrant differs from an ordinary search warrant only in that the judge authorizes the officers executing the warrant to wait for a limited period before notifying the subject of the search because immediate notice would have an “adverse result,” as defined by statute. As explained in three recent letters to Chairman Specter (attached), section 213 is an invaluable tool in the war on terror and our efforts to combat serious criminal conduct. In passing the USA PATRIOT Act, Congress recognized that delayed-notice search warrants are a vital part of the Department’s strategy of detecting and incapacitating terrorists, drug dealers, and other criminals before they can harm our Nation’s citizens. A delayed-notice search warrant is an important, though rarely used, tool. Delayed-notice warrants under section 213 represent less than 0.2% of all warrants authorized in the period of time between the enactment of the USA PATRIOT Act and January 31, 2005. As in the case of the other provisions of the Act, there have been no verified abuses of this authority.

It is false to suggest, as some have done, that a delayed-notice search warrant allows the Government to search an individual’s house, papers, and effects without notifying the individual of the search. In every case in which the Government executes a criminal search warrant, including those issued pursuant to section 213, the subject is told of the search. With a delayed-notice warrant, such notice is simply delayed for good cause and only for a reasonable period of

time—a time period defined by a Federal judge who is familiar with the specific facts and circumstances of the investigation.

Both the House and the Senate would amend section 213 to place limits on the length of time notice could be delayed or extensions granted. The Senate would set an initial delay period of seven days, unless the facts of the case justified a longer delay, with extensions of up to 90 days available unless the facts of the case justified a longer extension, while the House would allow initial delay of up to 180 days with extensions of up to 90 days available. Given the proven track record of success in the use of this provision, and the absence of abuse, we do not agree that section 213 needs amending, although we would not oppose imposing some presumptive limit on the length of time notice could be delayed or extensions granted. We are, however, concerned that judges would view the Senate provision as providing for a strong presumption in favor of requiring notice within seven days. This could force investigators to choose between either conducting a search and having to give notice prematurely—thereby jeopardizing ongoing investigations, endangering potential witnesses, or risking other adverse effects—or else not conducting the search at that time. We therefore would urge the Senate to recede to the House on this amendment.

#### **USA PATRIOT Act Section 215**

**Senate version, section 7. USA PATRIOT Act Section 215; Procedural Protections for Court Orders to Produce Records and Other Items in Intelligence Investigations; House version, section 107. Access to Certain Business Records Under Section 215 of the USA PATRIOT Act.** Section 215 of the USA PATRIOT Act amended the FISA business records provision to give the FISA Court the authority in foreign intelligence investigations, such as those involving international terrorism and espionage, to order the production of the same kinds of documents that prosecutors have always been able to obtain through grand jury subpoenas. The Department supports clarifying that the appropriate standard for a section 215 order is relevance; that a recipient of an order may disclose receipt of a section 215 order under certain circumstances; and that a recipient may seek judicial review of the production order in the FISA Court. However, we are concerned that the amendments to section 215's nondisclosure requirement that appear in both the House and Senate versions may lack needed safeguards with respect to disclosure to necessary persons and counsel. The amendments might allow disclosure to all manner of third parties, without any requirement that the Government be informed of the disclosure or have the ability to challenge the necessity of a given disclosure or the amount of information disclosed.

One could well imagine how the absence of any limits on disclosure to necessary persons or counsel could seriously risk dangerous disclosure of sensitive national security information. For example, suppose a company that has outsourced its data-center operations to a country for whom the United States is a prime espionage target, or entered into a joint venture with another company from such a country, is the recipient of a section 215 order. If the initial recipient of the section 215 order feels that he needs to inform the data-center or joint-venture personnel of the request in order to comply with the request, then before the Government knows it or can prevent it, unvetted foreign nationals will know what information is being sought. And in many instances, those other individuals, including the foreign nationals, may not really have a need to



know this information or could be given limited amounts of information and still comply with the request. Moreover, without a requirement that the recipient inform the Government before making such a disclosure, the Government will not have an opportunity to object to the disclosure or otherwise safeguard the integrity of ongoing investigations. These same concerns also apply in full force to the proposed amendments to the National Security Letter authorities discussed below. The Department of Justice would appreciate the opportunity to work with the conferees on this issue.

We are also deeply concerned about certain additional provisions in section 7 of the Senate bill, and we strongly encourage the Senate to recede to the House's amendments to section 215, provided that the nondisclosure amendments are refined to account for the lack of limits on disclosures to necessary persons. For example, the Senate amendments to section 215 would not only make the relevance standard explicit, but would require investigators to make a showing as to the likely relationship between the items sought and a foreign power or agent of a foreign power. We are concerned that the FISA Court will construe this amendment to substantially increase the burden that must be met to obtain items through a section 215 order. The amendment would likely make it more difficult to obtain materials through a section 215 order than through a grand jury subpoena, even though a section 215 order is accompanied by greater procedural protections, such as prior court approval, than pertain to a grand jury subpoena. Moreover, the Senate would vest the FISA Court judge with discretion to order disclosure of its order and related materials, potentially putting highly sensitive national security information at risk. Disclosure is a slippery slope, and tremendous care must be taken so as not to disclose — even inadvertently — sources and methods. In balancing interests, these national security interests far outweigh those of the record holder. The procedure for judicial review in the House bill is also preferable, as it provides for an initial review of a petition by the Presiding Judge and specifies that petitions shall be reviewed by one of the judges comprising a new petition review panel. The House version's provisions therefore would allow for expedited resolution of petitions by judges familiar with the FISA process and the review procedure.

Finally, section 7 would significantly amend the current section 215 reporting requirements, calling for more reporting to Congress of section 215 requests, with the reported information broken down by the type of entity from which records or tangible things were requested. For example, library, firearm, health, and taxpayer return information would be discretely listed. Section 7 requires this information to be submitted in unclassified form, although it may include a classified annex. This level of detail is burdensome to track, develop, and produce, and could also have the unintended effect of providing useful information to our enemies. Additional details simply make it easier for our enemies to decipher what we are doing to thwart them, and therefore should not be provided in an unclassified format.

#### **USA PATRIOT Act Section 505**

**Senate version, section 8. USA PATRIOT Act Section 505; Procedural Protections for National Security Letters; House version, sections 116-119. Judicial Review of National Security Letters; Confidentiality of National Security Letters; Violations of Nondisclosure Provisions of National Security Letters; Reports.** For years, the law has allowed Federal officials to issue National Security Letters (NSLs) to obtain specific types of important



information from certain third parties in national security investigations. By using an NSL, law enforcement was able to obtain information faster than with any other available tool, while simultaneously protecting sensitive information and the ongoing investigation. There are several NSL authorities, and the House bill would amend all but one of them, while the Senate would amend only the NSL authority in the Electronic Communications Privacy Act, 18 U.S.C. § 2709. Both the House and the Senate bills would make the following amendments: (1) clarify that a recipient may seek judicial review of an NSL; (2) clarify that a recipient may disclose receipt of an NSL to an attorney and to persons necessary for compliance; (3) explicitly provide for judicial review of a nondisclosure requirement; and (4) explicitly allow the Government to move for judicial enforcement of non-compliance by recipients. Due to differences in drafting, as well as the fact that the House would amend each of the relevant authorities, we strongly support sections 116-119 of the House bill.

For example, the Senate bill would allow for judicial review of an NSL production request or nondisclosure requirement in “an appropriate” United States District Court. The failure to specify the district court with jurisdiction would lead, we believe, to forum shopping, confusion over jurisdiction, and litigation. Second, although section 8 of the Senate bill provides that the Attorney General may seek enforcement of a request for production, it does not explicitly provide for contempt penalties in the absence of compliance. Third, section 8 lacks criminal penalties for violating nondisclosure requirements. Fourth, there is no requirement in the Senate bill that challenges to either the production request or the nondisclosure requirement be filed under seal, creating a substantial risk that sensitive national security information would be disclosed through the filing of a petition for review.

Similarly, although section 8 of the Senate bill allows for limiting disclosure of information in proceedings consistent with the requirements of the Classified Information Procedures Act (CIPA), it does not require a court or litigants to take any steps to protect this sensitive national security information. Finally, it is difficult to imagine how CIPA would apply to these petitions for review, which would be civil proceedings. CIPA currently applies in the criminal context, to protect the due process rights of an accused, and relies on constitutional and statutory principles that apply only in the criminal context. The civil context simply does not function under the same rules.

The Department believes that the language in the House bill accomplishes the same goals—without raising the same concerns—as the Senate bill, and we urge the Senate to recede to the House on this issue. We would also appreciate the opportunity to work with the conferees to address our concern that the amended nondisclosure requirement might lack necessary safeguards, as explained with respect to section 215.

### **Sunsets**

We applaud the House and the Senate for making permanent 14 out of 16 sunset provisions as well as the sunset material support amendment in the Intelligence Reform and Terrorism Prevention Act of 2004. We further applaud the House for making permanent section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004—the “lone wolf” provision. Both the House and the Senate, however, would impose additional sunsets on

important provisions of the USA PATRIOT Act, and the Senate would impose a new sunset on the “lone wolf” provision. The House bill would provide for new ten-year sunsets on USA PATRIOT Act sections 206 and 215, and the Senate bill would provide for new four-year sunsets on the same provisions and the “lone wolf” provision. We oppose additional sunsets on these provisions, but in the event that sunsets are retained, we strongly encourage the Senate to recede to the House on the issue of sunsets.

The Department of Justice has an unblemished track record in the use of these provisions that demonstrates their utility and proves that the judicial and congressional checks already built into the USA PATRIOT Act are effective. There has been extensive oversight of and debate about the Act, including 18 congressional hearings with 32 Department witnesses. The oversight and debate have confirmed that there have been no verified abuses of the USA PATRIOT Act. With this established track record, the purpose behind the sunsets—to allow Congress to consider the Department’s use of the provisions—has been fulfilled. There is no further legitimate justification to support additional sunsets. Moreover, sunsets on critical investigatory tools are highly unusual and discourage investigators from investing time and resources into understanding those tools and maximizing their utility. We therefore do not support these additional sunsets. At the very least, there is no reason to set short-term sunsets of four years as opposed to the ten-year period provided by the House bill.

Some appear to believe that sunsets are necessary for oversight. As the Attorney General has testified: “The Department of Justice has exercised care and restraint in the use of these important authorities, because we are committed to the rule of law. We have followed the law, because it is the law, not because it is scheduled to sunset. With or without sunsets, our dedication to the rule of law will continue. The Department will strive to continue to carry out its work lawfully and appropriately, and as a citizen I expect Congress will continue its active oversight over our use of the USA PATRIOT Act, not because it sunsets, but because oversight is a constitutional responsibility of Congress.” We urge the conferees to resolve this issue based on the facts—the absence of a single verified abuse of these important provisions.

### **Terrorism-Related Grant Programs**

We applaud the House for replacing Section 1014 of the USA PATRIOT with an amendment to the Homeland Security Act of 2002 (“HSA”), providing much-needed improvements to how the Federal government supports State and local homeland security efforts. This revision brings the statutory responsibility for homeland security grants in line with current policy and practice. The Department of Justice understands that the Secretary of Homeland Security supports enactment of “Title XVIII -- Funding for First Responders,” enhancing his grant authorities under the HSA.

### **Additional Reporting Requirements**

The Department supports the oversight efforts of this Committee and others and makes every effort to facilitate that oversight. The Department is concerned, however, about the burden from and national security implications of the ever-increasing number of reporting requirements, particularly those that are public. For example, the Intelligence Reform and Terrorism

Prevention Act of 2004 includes some 106 different reporting requirements. The Homeland Security Act of 2002 includes more than 50 various reports—including many continuing reporting requirements—and the USA PATRIOT Act included more than 30. Pursuant to the Foreign Intelligence Surveillance Act, the Attorney General is already required to submit reports to Congress that include the following information (although this is by no means a comprehensive list):

- The aggregate number of persons targeted for orders issued under this chapter, including a breakdown of those targeted for electronic surveillance under section 1805 of this title; physical searches under section 1824 of this title; pen registers under section 1842 of this title; and access to records under section 1861 of this title. *See* 50 U.S.C. § 1871.
- The total number of applications made for orders and extensions of orders approving electronic surveillance under this subchapter; and the total number of such orders and extensions either granted, modified, or denied. *See* 50 U.S.C. § 1807.
- A description of each criminal case in which information acquired under this chapter has been passed for law enforcement purposes during the period covered by such report; and each criminal case in which information acquired under this chapter has been authorized for use at trial during such reporting period. *See* 50 U.S.C. § 1808.
- The total number of applications made for orders approving physical searches under this subchapter; the total number of such orders either granted, modified, or denied; and the number of physical searches which involved searches of the residences, offices, or personal property of United States persons, and the number of occasions, if any, where the Attorney General provided notice pursuant to section 1825(b) of this title. *See* 50 U.S.C. § 1826.
- The total number of applications made for orders approving the use of pen registers or trap and trace devices under this subchapter [50 U.S.C.A. § 1841 *et seq.*]; and the total number of such orders either granted, modified, or denied. *See* 50 U.S.C. § 1846.
- The total number of applications for orders approving requests for the production of tangible things under section 1861 of this title; and the total number of such orders either granted, modified, or denied. *See* 50 U.S.C. § 1862.
- A summary of significant legal interpretations of this chapter involving matters before the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review, including interpretations presented in applications or pleadings filed with the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review by the Department of Justice. *See* 50 U.S.C. § 1871.
- Copies of all decisions (not including orders) or opinions of the Foreign Intelligence Surveillance Court or Foreign Intelligence Surveillance Court of Review that include significant construction or interpretation of FISA. *See* 50 U.S.C. § 1871

All of the above information is reported to Congress in a manner consistent with the national security. This ensures that the public is informed through its representatives without aiding our enemies. If public disclosures occur often enough through reporting requirements, and with enough detail, terrorist and foreign intelligence organizations will discern our sources, methods, and capabilities, and thereby adjust their own activities to avoid detection and successfully thwart our efforts. If they succeed, we will be far less likely to prevent further exposure of our Nation's secrets, and we will be at greater risk of attack. Indeed, in this sophisticated war over information, even innocuous disclosures can be extremely damaging to the national security if a foreign power can create, by combining our public disclosures with other information that they glean from clandestine and other sources, a mosaic of our intelligence operations.

In addition, all reporting requirements, not just public ones, impose substantial costs and can be very burdensome to administer. For instance, multiple Office of Intelligence Policy and Review attorneys—not staff assistants—worked for weeks to compile and ensure the accuracy and completeness of the 88-page FISA Semi-Annual Report to Congress before it was transmitted on July 1, 2005, as was the case for every Semi-Annual Report that the Department has filed on a twice-yearly basis with Congress. While reporting is an important aspect of oversight, particularly in the FISA context, preparing this complex report requires these attorneys to divert their time and attention from reviewing and processing FISA applications.

We have been discouraged to learn how few Members are even aware of this detailed report, much less avail themselves of the opportunity to review it. Because the document contains such sensitive information, it is highly classified. However, it is our understanding that any Member and staff with appropriate security clearances and a need to know may review the Semi-Annual Report. We strongly encourage any Member interested in this subject to review the Semi-Annual Report and the information already provided to the Congress, in this report as well as in the similarly exhaustive and detailed Semi-Annual Reports that have been filed twice a year in the past, before imposing additional reporting requirements.

Nor do we believe that multiple reporting requirements are the best method to ensure effective congressional oversight. Congress has held 18 hearings with 32 Department witnesses before four Committees concerning the reauthorization of the USA PATRIOT Act. The Department has answered hundreds of direct questions and thousands of informal oral requests, responded to hundreds of questions for the record, provided hundreds of briefings, transmitted voluminous amounts of informative documents and written numerous letters to satisfy Members' specific requests and concerns. Many Members of Congress who are focused on a particular issue request customized information from the Department. Because these requests are tailored to a particular Member's concerns, they are a better form of congressional oversight than generic reporting, which is often burdensome to compile and can be misconstrued because of its general nature.

For these reasons, although we respect Congress's important oversight role, we are concerned about the ever-increasing number of reporting obligations.

**Additional Provisions in Title I of the House Version of H.R. 3199:**  
**USA PATRIOT and Terrorism Prevention Reauthorization Act**

We applaud the efforts of the House to improve our ability to combat terrorism and other serious crimes with its additional amendments in Title I. However, we want to offer a few technical comments on some of the additional provisions.

**Section 110. Prohibition on Planning Terrorist Attacks on Mass Transportation;**  
**Section 115. Attacks Against Railroad Carrier and Mass Transportation Systems.** We support sections 110 and 115; however, we note that section 110 would be moot if section 115 is also enacted. The conferees may wish to consider conforming the language in section 115 to include the language added by section 110.

**Section 112. Adding Offenses to the Definition of “Federal Crime of Terrorism.”**  
We support this provision but note that paragraph (2) is unnecessary, as 18 U.S.C. § 832 was added to 18 U.S.C. § 2332b(g)(5)(B) by section 6803(b)(3) of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458.

**Section 113. Wiretap Predicates.** We support the addition of wiretap predicate offenses, but note that, with respect to paragraphs (a)(3) and (4), sections 1361, 1362, 1363, 1364, 2155, 2156, 2280, and 2281 are already wiretap predicate offenses.

**Section 120. Definition for Forfeiture Provision Under Section 806 of the USA PATRIOT Act.** This provision would narrow the potential predicate offenses for terrorism-related forfeiture under 18 U.S.C. § 981(a)(1)(G) by replacing the cross-reference to 18 U.S.C. § 2331 (which broadly and generically defines acts of domestic and international terrorism as certain types of activities “that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State”) with a cross-reference to 18 U.S.C. § 2332b(g)(5)(B), which defines only certain specific Federal criminal offenses as “Federal crimes of terrorism” if they are “calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct.”

We are concerned that this amendment would unduly restrict the scope of the terrorism forfeiture statute by, among other things, excluding State law offenses and foreign law offenses that constitute an “act of domestic or international terrorism” within the meaning of 18 U.S.C. § 2331. If the intention of the drafters of this provision was to exclude certain particular violations from the scope of section 981(a)(1)(G), it would be more appropriate to specify those exclusions rather than making this proposed major change in scope.

Moreover this provision is incomplete. The forfeiture provision to which the proposed new cross-reference would apply, 18 U.S.C. § 981(a)(1)(G), repeatedly employs the term used in the currently cross-referenced section, 18 U.S.C. § 2331, “act of domestic or international terrorism.” That term does not appear in the proposed new cross-reference, section 2332b(g)(5)(B). Therefore, if the cross-reference is replaced, the term “act of domestic or international terrorism” in 981(a)(1)(G) must be changed each time it appears to “Federal crime

of terrorism,” the term defined in 2332b(g)(5). In addition, the new cross-reference proposed by section 120 should be to the entire definition of “Federal crime of terrorism,” *i.e.*, section 2332b(g)(5). The proposed cross-reference, subsection 2332b(g)(5)(B), only lists violations that become “Federal crimes of terrorism” if one of the intent elements set forth in 2332b(g)(5)(A) (*i.e.*, that the violation is calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct) is shown.

**Section 122. Interception of Communications.** We support this provision, but note that parts of paragraphs (1)(B) and (1)(C) are unnecessary, as 18 U.S.C. §§ 832 and 930 are being added as wiretap predicates by section 113 of the bill.

**Section 123: Penal Provisions Regarding Trafficking in Contraband Cigarettes or Smokeless Tobacco.** This provision would make various amendments to 18 U.S.C. §§ 2341 *et seq.*, dealing with contraband cigarettes. Among other things, it would amend the contraband cigarette forfeiture provision, 18 U.S.C. § 2344(c), by adding “contraband smokeless tobacco” to the forfeitable items, by removing the current reference to Internal Revenue Code procedures without inserting any other procedural cross-reference (*i.e.*, to Civil Asset Forfeiture Reform Act of 2000 (“CAFRA”) procedures under 18 U.S.C., chapter 46), and by adding that any contraband cigarettes or smokeless tobacco shall be either destroyed and not resold, or used for undercover investigative operations and then destroyed and not resold.

We support section 123 to the extent that it deletes the outdated reference to Internal Revenue Code forfeiture provisions, which no longer apply in light of the enactment of CAFRA. *See* 18 U.S.C. § 983(i) (defining “civil forfeiture statutes” covered by CAFRA to cover all civil forfeitures except forfeitures under specific provisions, not including section 2344(c)); 18 U.S.C. § 3051(c) (CAFRA applies to civil forfeitures administered by ATF, except as provided in section 983). However, we suggest that the conferees consider also replacing the outdated IRC procedural reference with a clear reference to CAFRA procedures, by ending the first sentence of current section 2344(c) with “seizure and forfeiture”, and inserting thereafter the following: “The provisions of chapter 46 of title 18 relating to civil forfeitures shall extend to any seizure or civil forfeiture under this section.” The language to be added by subsection (d) should be amended by starting the sentence after this insertion with: “Any cigarettes or smokeless tobacco so seized and forfeited . . . .”

We would also note our concern that making the minimum threshold for Contraband Cigarette Trafficking Act (“CCTA”), 18 U.S.C., chapter 114, 10,000 cigarettes could bring legitimate personal use purchasers, who are a low enforcement priority, within the scope of the CCTA. Accordingly, we suggest, as an alternative, a threshold of 30,000 cigarettes. This would achieve the goal of lowering the threshold while also suggesting a quantity well above personal use. And while we applaud the expansion of CCTA recordkeeping requirements, which presently apply only to limited information about the purchaser of cigarettes and are inadequate for enforcement purposes, we are concerned that the amendment would exempt “retail purchaser” from these recordkeeping requirements. As neither the CCTA nor section 123 defines the term “retail purchaser,” organized criminals, who often convey the appearance of lawful retail purchasers, could turn the absence of such a definition into a loophole. We therefore suggest either deleting the exemption or making it clear that a retail purchase for

purposes of this provision is one who is clearly purchasing a personal use quantity, e.g., two cartons.

**Section 124. Prohibition of Narco-Terrorism.** This provision would add new section 1010A to Part A of the Controlled Substance Import and Export Act (codified at 21 U.S.C. § 951 *et seq.*) to create a specific offense for “narco-terrorists who aid and support terrorists or foreign terrorist organizations.” We support this provision but recommend that the new offense should be made a forfeiture and money-laundering predicate. The proposed new section 1010A created by this section would not be a “Federal crime of terrorism” as defined in 18 U.S.C. § 2332b(g)(5), and therefore would not be a forfeiture predicate for section 981(a)(1)(G), if that section is amended as proposed in section 120 of the bill. If the new section 1010A fell within Subchapter II of Title 21, Chapter 13, it would be a predicate for criminal forfeiture only under 21 U.S.C. § 853. We would have no objection to the inclusion of new section 1010A within the offenses listed in 18 U.S.C. § 2332b(g)(5)(B), which would also alleviate our concern about the new section not being a forfeiture and money-laundering predicate. The provision also refers to “a controlled substance, *flunitrazepam*, or listed chemical” (emphasis added). We recommend deleting Flunitrazepam from this provision, as it is a controlled substance. 21 CFR 1308.14(c)(21).

**Section 132. Report by Attorney General (Data Mining).** Section 132 would require a detailed report to Congress, with yearly updates, for each agency that “use[s]” or “develop[s]” a “data-mining technology.” Under section 132(a)(2), each report would be required to meet eight detailed and broad-ranging requirements, such as “[a] thorough discussion of the plans for the use of [data-mining] technology” and “[a] list and analysis of the laws and regulation that govern the information to be collected, reviewed, gathered, and analyzed with the data-mining technology and a description of any modifications of such laws that will be required to use the information in the matter proposed under such program.” We have repeatedly objected to “burdensome reporting requirements” and other similar congressional attempts to micromanage the work of the Executive branch. *See The Constitutional Separations of Powers Between the President and Congress*, 20 Op. O.L.C. 124, 135, 180-81 (1996). The report envisioned by section 132 would be particularly onerous, as it would require the Attorney General to provide information, not only on the activities of the Department of Justice, but also on the activities of every other agency of the Federal government that may engage in “data mining.” Gathering this information would require a significant diversion of resources from other essential functions and would be unlikely, in any event, to be accomplished within 180 days. As a consequence, we strongly urge that the House recede to the Senate regarding this matter and that section 132 not be included in the conference report. At the very least, we encourage the conferees to limit the requirement to a one-time reporting obligation concerning Department of Justice activities only.

If, however, section 132 is retained, we have several other concerns about the provision as it is currently drafted. In particular, section 132(b)(1) defines “data-mining” so ambiguously that it could be read to require reports to Congress for routine law enforcement procedures. “Data-mining” is defined as a query run on any database that “was obtained from or remains under the control of a non-Federal entity,” so long as the query “does not use a specific individual’s personal identifiers” and “is conduct[ed]” by a department or agency “to find a pattern indicating terrorist or other criminal activity.” That definition appears to constitute an



attempt to focus on so-called “pattern-based data-mining,” rather than so-called “subject-based data-mining.” (Pattern-based data-mining seeks patterns in data that might indicate certain behaviors without using subject-specific information as a predicate for the search; subject-based data-mining returns results connected in some way to some inputted information about a suspected subject.)

We believe that the definition used in the statute is ambiguous in two important ways, at least one of which vitiates its apparent intent to single out pattern-based data-mining. First, “database” is not defined, except to exclude certain discrete compilations of information such as telephone directories or “databases of judicial and administrative opinions.” And although the statute specifically excludes Internet sites and information available to the public without a fee, this definition would nonetheless include many databases useful for intelligence and law enforcement, such as State DMV databases. Given the myriad fees associated with Internet use, what constitutes “information publicly available via the Internet *without payment of a fee*” could also be confusing.

Second, the definition of “data-mining” is ambiguous because the term “specific individual’s personal identifiers” is undefined. It is unclear, for example, whether telephone numbers, license plate numbers, workplaces, and even cities of residence would constitute “personal identifiers.” Because section 132 requires a report to Congress when data-mining queries do not “use” these “specific personal identifiers,” the scope of the reporting obligation would be unclear. Consequently, many routine criminal and intelligence investigative procedures—such as determining who owns a car with a particular license plate, who owns a particular telephone number, or what computer corresponds with a particular IP address—could potentially constitute a “data-mining technology” that would require a report to Congress. We believe the qualifier in section 132(b)(1)(B) should therefore be clarified to ensure that queries that are subject-based but do not involve inputs that appear on their face to be personally identifiable nonetheless fall outside the bounds of this reporting requirement.

In addition, section 132(a)(2)(E) requires a “list and analysis of the laws and regulations that govern the information to be collected, reviewed, gathered, and analyzed with the data-mining technology.” This requirement is not limited to those “laws and regulations” that are actually relevant to the data-mining technology or to use of the information for law enforcement or intelligence purposes; rather, it includes *all* laws and regulations that govern the information in question. We believe the requirement should be limited to laws and regulations relevant to the information’s use for data-mining for law enforcement or intelligence purposes.

Section 132(a)(2)(F)(ii) requires the agency or department to discuss the policies used to “ensure that only accurate information is collected and used.” Because many of the databases described in the section are not under Federal control, we believe it would be more appropriate and useful to require a discussion of policies to “ensure that only accurate information is collected and used or account for the possibility of inaccuracy in that information and guard against harmful consequences of potential inaccuracies.” Similarly, section 132(a)(2)(G) appears to presume that the Federal government or some other actor will notify all individuals whose personal information is “used in the data-mining technology” and allow them to opt out. Because many of the databases described in the section are not under Federal control, in which



case the Federal government will have no way of knowing the universe of persons whose information is contained in those databases, and because in any event the entities who hold the relevant information may be under no legal obligation to provide the notice discussed, we believe that the concern apparently underlying this reporting requirement would be more effectively dealt with, if at all, through other means. We also believe section 132(a)(3)(B) should explicitly allow for the possibility that agencies or departments may cease to engage in data-mining activities and thus no longer be required to provide annual updates through the Attorney General.

Section 132(a)(2)(H) would require that the report include “[a]ny necessary classified information in an annex that shall be available to the Committee on the Judiciary of both the Senate and the House of Representatives.” The Supreme Court has observed that the authority to control access to national security information “flows primarily from [the] constitutional investment of power in the President and exists quite apart from any explicit congressional grant.” *Dep’t of Navy v. Egan*, 484 U.S. 518, 527 (1988). Although the President does, as a matter of comity, often provide some classified information to portions of the Congress where he considers doing so consistent with national security, a requirement of blanket disclosure to the committee of classified information, as this section could be construed to require, could jeopardize national security and contravene the President’s “authority to protect such information . . . as head of the Executive Branch and as Commander in Chief.” *Id.* at 527. To avoid unconstitutionally intruding on the President’s authority to control access to national security information, we recommend clarifying, consistent with longstanding practice in this area, that the President may withhold classified information if he determines that its production would jeopardize national security (e.g., adding at the end of section 132(a)(2)(H) “consistent with national security”).

Overall, we are concerned that this flawed reporting requirement could do more harm than good in this increasingly important area and we urge the House to recede to the Senate on this issue.

## **Title II of the House Version of H.R. 3199: Terrorist Death Penalty Enhancement**

This Administration has consistently supported strengthening the penalties for crimes of terrorism, and therefore we support this Title. We simply would make two recommendations with respect to these provisions.

**Section 211. Terrorist Offenses Resulting in Death.** To make this section (and section 212) workable, we suggest that the phrase “Federal crime of terrorism as defined in section 2332b(g)(5)(B)” be replaced with “crime as specified in section 2332b(g)(5)(B),” because a defendant is never convicted of a “Federal crime of terrorism.” A defendant is convicted of one of the offenses listed in section 2332b(g)(5)(B). The trier of fact does not make a determination of the “motive” specified in section 2332b(g)(5)(A).

**Section 213. Death Penalty Procedures in Air Piracy Cases.** We recommend that the current text of this provision be designated as subsection (a) and that a new subsection (b) be added, as follows: “(b) Severability Clause.— If any provision of the section 60003(b)(2) of the

Violent Crime and Law Enforcement Act of 1994, Pub. L. No. 103-322, or the application thereof to any person or any circumstance is held invalid, the remainder of such section and the application of such section to other persons or circumstances shall not be affected thereby.”.

**Title III of the House Version of H.R. 3199:**  
**Reducing Crime and Terrorism at America’s Seaports**

We support the goal of strengthening our security and reducing crime and terrorism at our seaports. We do have a few concerns regarding section 313 as it currently is drafted. First and foremost, this provision appears to be duplicative of existing export control laws and would therefore be unnecessary at best. For example, an indictment for smuggling under this provision that also included a charge under another export control statute, such as the Arms Export Control Act, might be found by a court to be multiplicitous. In addition, the amendment could upset existing agreements between investigative agencies with enforcement responsibilities in this area without conferring any benefits in terms of prosecutions. We also have additional concerns relating to section 313 specifically.

**Section 313. Smuggling Goods from the United States.** Section 313(d) provides for civil forfeiture for violations of proposed section 554, via an amendment to existing 19 U.S.C. § 1595a. However, the provision neglects to include “seizure,” as it should, to make it parallel to the existing subsections of section 1595a. The provision is also confusingly drafted in a way likely to be construed as limiting facilitating property to items that facilitated *preparations* for the illegal sending or exportation, but not the illegal sending or exportation, or attempted sending or exportation, itself. We recommend that the conferees make the changes noted in bold below:

(d) Tariff Act of 1990—Section 596 of the Tariff Act of 1930 (19 U.S.C. § 1595a) is amended by adding at the end the following:

“(d) Merchandise exported or sent from the United States or attempted to be exported or sent from the United States contrary to law, or the proceeds or value thereof, and property used to facilitate the **exporting or sending of such merchandise, the attempted exporting or sending of such merchandise, or the** receipt, purchase, transportation, concealment, or sale of such merchandise prior to exportation shall be **seized and** forfeited to the United States.”.

**Title IV of the House Version of H.R. 3199: Combating Terrorism Financing**

As this Administration has consistently explained, our strategy must include prevention at the earliest possible stage—stopping a terrorist with a hand on the checkbook rather than a hand on a trigger. We therefore support the provisions of Title IV, with two recommendations.

**Section 406. Technical Amendments to USA PATRIOT Act.** Section 406(b) codifies section 316 of the USA PATRIOT Act by adding a new section 18 U.S.C. § 987 that would provide various protections for an “owner of property that is confiscated under this chapter or any other provision of law relating to the confiscation of assets of suspected international

terrorists.” The provision is confusingly drafted. Among other things, it returns to pre-CAFRA law as to the burdens of proof, but then provides in a “savings clause” that CAFRA’s “remedies” also apply. We recommend replacing the proposed section 987 with language attached as Appendix A attached hereto.

Section 316 of the USA PATRIOT Act included a provision reversing the burden of proof in civil forfeiture cases brought against the assets of suspected international terrorists, and providing that reliable hearsay could be admitted into evidence in such cases. Thus, if the Government brings a forfeiture action under 18 U.S.C. § 981(a)(1)(G) (enacted by section 806 of the USA PATRIOT Act), the burden would be on the property owner to prove, as an affirmative defense, that he was not “engaged in planning or perpetrating acts of terrorism against the United States, its citizens or their property,” and that the property therefore was not subject to forfeiture under the statute. Section 316 also included a subsection (c) that was intended to make clear that notwithstanding the reversal of the burden of proof, all other procedural protections included in Chapter 46 of title 18, including the reforms enacted by the CAFRA, would apply. At the same time, this subsection was intended to make clear that if an action is brought to confiscate a terrorist’s assets under a statute exempted from CAFRA—such as the International Emergency Economic Powers Act (50 U.S.C. § 1705) (IEEPA), which is exempted from CAFRA by section 983(i)—the property owner would nevertheless be able to assert the innocent owner defense codified at 18 U.S.C. § 983(d), and to contest the forfeiture under the Administrative Procedure Act. The language proposed in Appendix A codifies section 316 by placing it in title 18, and by redrafting subsection (c) to set forth the clarifications more clearly and concisely.

**Section 410. Designation of Additional Money Laundering Predicate.** We support this provision, which would add 18 U.S.C. § 2339D as a money laundering predicate to 18 U.S.C. § 1956(c)(7)(D), but note that section 403 of the bill would also add § 2339C to § 1956(c)(7)(D). If section 403 is enacted, then section 410 should place 2339D after 2339C.

**Appendix A**

**1. (b) CODIFICATION OF SECTION 316 OF THE USA PATRIOT ACT.**

(1) Chapter 46 of title 18, United States Code, is amended –

(A) in the chapter analysis, by inserting at the end the following:

“987. Anti-terrorist forfeiture protection.”; and

(B) by inserting at the end the following:

**“§ 987. Anti-terrorist forfeiture protection**

**“(a) Right to contest.** – An owner of property that is ~~confiscated~~ **the subject of an action** under this chapter or any other provision of law relating to the confiscation of assets of suspected international terrorists, may contest that ~~confiscation~~ **action** by filing a claim in the manner set forth in the Federal Rules of Civil Procedure (Supplemental Rules for Certain Admiralty and Maritime Claims), and asserting as an affirmative defense that –

“(1) the property is not subject to confiscation under such provision of law; or

“(2) the innocent owner provisions of section 983(d) apply to the case.

**“(b) Evidence.** – In considering a claim filed under this section, a court may admit evidence that is otherwise inadmissible under the Federal Rules of Evidence, if the court determines that the evidence is reliable, and that compliance with the Federal Rules of Evidence may jeopardize the national security interests of the United States.

**~~“(c) Clarifications.—~~**

~~“(1) Protection of rights.—The exclusion of certain provisions of Federal law from the definition of the term ‘civil forfeiture statute’ in section 983(i) shall not be construed to deny an owner of property the right to contest the confiscation of assets of suspected international terrorists under—~~

~~“(A) subsection (a) of this section;~~

~~“(B) the Constitution; or~~

~~“(C) subchapter II of chapter 5 of title 5, United States Code (commonly known as the ‘Administrative Procedure Act’).~~

~~“(2) Savings clause.—Nothing in this section shall limit or otherwise affect any other remedies that may be available to an owner of property under section 983 or any other provision of law.”.~~

**“(c) Clarifications.** (1) Except as provided in (a) and (b), in any action to confiscate the assets of suspected international terrorists pursuant to a civil forfeiture statute, as defined in Section 983(i), the procedures set forth in this Chapter regarding civil forfeiture actions shall apply.

“(2) In any action to confiscate the assets of suspected international terrorists pursuant to a statute other than a civil forfeiture statute, as defined in Section 983(i), the owner of the property may contest the action as provided in (a) and/or pursuant to subchapter II of

chapter 5 of title 5, United States Code (commonly known as the 'Administrative Procedure Act').”

(2) Subsections (a), (b), and (c) of section 316 of Pub. L. 107-56 are repealed.



U.S. Department of Justice

Office of Legislative Affairs

RECEIVED

2005 JUL -5 AM 11: 57

Office of the Assistant Attorney General

Washington, D.C. 20530

~~SECRET~~

OIPR  
DEPT OF JUSTICE

MAY 24 2005

Senator Pat Roberts, Chairman  
Select Committee on Intelligence  
United States Senate  
Washington, DC 20510

Dear Chairman Roberts:

I write to express the Department of Justice's strong opposition to any attempt to impose an "ascertainment" requirement on the implementation of multi-point or "roving" surveillance conducted under the Foreign Intelligence Surveillance Act (FISA). (U)

As the Members of this Committee are well aware, a roving surveillance order attaches to a particular target rather than to a particular phone or other communications facility. Since 1986, law enforcement has been able to use roving wiretaps to investigate ordinary crimes, including drug offenses and racketeering. Before the USA PATRIOT Act, however, FISA did not include a roving surveillance provision. Therefore, each time a suspect changed communication providers, investigators had to return to the FISA Court for a new order just to change the name of the facility to be monitored and the "specified person" needed to assist in monitoring the wiretap. However, international terrorists and spies are trained to thwart surveillance by regularly changing communication facilities, especially just prior to important meetings or communications. Therefore, without roving surveillance authority, investigators were often left two steps behind sophisticated terrorists and spies. (U)

Thankfully, section 206 of the USA PATRIOT Act ended this problem by providing national security investigators with the authority to obtain roving surveillance orders from the FISA Court. This provision has put investigators in a much better position to counter the actions of spies and terrorists who are trained to thwart

~~SECRET~~

Classified by:

James A. Baker, Counsel for Intelligence Policy,  
Office of Intelligence Policy and Review, U.S.  
Department of Justice

Reason:

1.4(c)

Declassify on:

X1

Declassified by James A. Baker  
Counsel for Intelligence Policy  
OIPR/USDOJ  
Date: 7/9/05

~~SECRET~~

surveillance. This is a tool that we do not use often, but when we use it, it is critical. As of March 30, 2005, it had been used 49 times and has proven effective in monitoring foreign powers and their agents. (U)

Some in Congress have expressed the view that an "ascertainment" requirement should be added to the provisions in FISA relating to "roving" surveillance authority. Section 2 of the S. 737, the Security and Freedom Ensured Act of 2005 ("SAFE Act"), for example, would provide that such surveillance may only be conducted when the presence of the target at a particular facility or place is "ascertained" by the person conducting the surveillance. (U)

Proponents of the SAFE Act have claimed that this provision would simply impose the same requirement on FISA "roving" surveillance orders that pertains to "roving" wiretap orders issued in criminal investigations, but this is wholly inaccurate. The relevant provision of the criminal wiretap statute states that the roving interception of oral communications "shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order." See 18 U.S.C. § 2518(12). With respect to the roving interception of wire or electronic communications, however, the criminal wiretap statute imposes a more lenient standard, providing that surveillance can be conducted "only for such time as it is reasonable to presume that [the target of the surveillance] is or was reasonably proximate to the instrument through which such communication will be or was transmitted." See 18 U.S.C. § 2518(11)(b)(iv). (U)

Any "ascertainment" requirement, however, whether it is the one contained in the SAFE Act or the one currently contained in the criminal wiretap statute, should not be added to FISA. Any such requirement would deprive national security investigators of necessary flexibility in conducting sensitive surveillance. Due to the different ways in which foreign intelligence surveillance and criminal law enforcement surveillance are conducted as well as the heightened sophistication of terrorists and spies in avoiding detection, provisions from the criminal law cannot simply be imported wholesale into FISA. (U)

Targets of FISA surveillance are often among the most well-trained and sophisticated terrorists and spies in the world. As a result, they generally engage in detailed and extensive counter-surveillance measures. Adding an ascertainment requirement to FISA therefore runs the risk of seriously jeopardizing the Department's ability to effectively conduct surveillance of these targets because, in attempting to comply with such a requirement, agents would run the risk of exposing themselves to sophisticated counter-surveillance efforts. (U)

~~SECRET~~

~~SECRET~~

In addition, an ascertainment requirement is unnecessary in light of the manner in which FISA surveillance is conducted. As the Members of this Committee are no doubt aware, intercepted communications under FISA are often not subject to contemporaneous monitoring but rather are later translated and culled pursuant to court-ordered minimization procedures. These procedures adequately protect the privacy concerns that we believe the proposed ascertainment provisions are intended in part to address. (U)

While we understand the concern that conversations of innocent Americans might be intercepted through roving surveillance under FISA, the Department does not believe that an ascertainment requirement is an appropriate mechanism for addressing this concern. Rather, we believe that the current safeguards contained in FISA along with those procedures required by the FISA Court amply protect the privacy of law-abiding Americans. (U)

First, under section 206, the target of roving surveillance must be identified or described in the order of the FISA Court, and if the target of the surveillance is only described, such description must be sufficiently specific to allow the FISA Court to find probable cause to believe that the specified target is a foreign power or agent of a foreign power. As a result, section 206 is always connected to a particular target of surveillance. Roving surveillance follows a specified target from phone to phone and does not "rove" from target to target. (U)

Second, surveillance under section 206 also can be ordered only after the FISA Court makes a finding that the actions of the specified target may have the effect of thwarting the surveillance (by thwarting the identification of those persons necessary to assist with the implementation of surveillance). (U)

Additionally, all "roving" surveillance orders under FISA must include Court-approved minimization procedures that limit the acquisition, retention, and dissemination by the government of information or communications involving United States persons. These are usually in the form of standard minimization procedures applicable to certain categories of surveillance, but the procedures may be modified in particular circumstances. (U)

(b)(1)1.4c

~~SECRET~~



~~SECRET~~

(b)(1)1.4c

In sum, the Department believes that the safeguards set forth in this letter reflect the appropriate balance between ensuring the effective surveillance of sophisticated foreign powers and their agents and protecting the privacy of the American people. The Department strongly opposes any attempt to disturb this balance by adding an ascertainment requirement to the provisions of FISA relating to roving surveillance authority. (U)

We hope that this information will be useful to the Committee as it considers the reauthorization of those USA PATRIOT Act provisions scheduled to sunset at the end of this year. Please do not hesitate to contact me if you have additional questions or concerns about this issue. (U)

Sincerely,

*William E. Moschella*

William Moschella  
Assistant Attorney General

~~SECRET~~



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

July 13, 2005

The Honorable F. James Sensenbrenner, Jr.  
Chairman  
Committee on the Judiciary  
U.S. House of Representatives  
Washington, D.C. 20515

Dear Mr. Chairman:

We understand that issues have been raised about section 209 of the USA PATRIOT Act and that some may offer amendments to address misperceptions that certain electronic communications can be lawfully intercepted while they are "stored" for very short periods of time during transmission.

Such amendments are intended to reverse the now-withdrawn First Circuit decision in *United States v. Councilman*, 373 F.3d 197, *withdrawn by* 385 F.3d 792 (1st. Cir. 2004) (withdrawing panel opinion and granting rehearing en banc). In *Councilman*, the owner of an e-mail service provider allegedly configured its e-mail processing software to copy for its own commercial advantage all incoming messages from Amazon.com to the provider's customers. The provider obtained these messages contemporaneous with their receipt but while the messages were in "electronic storage" within the meaning of 18 U.S.C. § 2510(17). The owner was charged with violating the criminal provisions of the Wiretap Act ("title III"). Title III governs not only the access of private communications by criminals, as was alleged in *Councilman*, but also the court-approved, lawful access to private communications by law enforcement in criminal investigations. The *Councilman* panel opinion held that title III was not violated when e-mail messages were acquired while in "electronic storage," regardless of whether they were acquired contemporaneously with transmission.

We believe that the vacated *Councilman* decision was wrong, but we oppose any statutory amendment during the pendency of the *Councilman* appeal, which still is awaiting decision by the First Circuit *en banc*. We believe that the First Circuit is likely to reach the correct result in *Councilman*: that the interception of the e-mails contemporaneous with transmission violated title III. To this end, we agree with the amendment's sponsors, but strongly suggest that legislative action at this time is premature. Rest assured, if we were to get a negative opinion from the First Circuit *en banc* panel, we would – at that time – be willing to work with Congress to craft an appropriate solution.

Any legislation enacted before *Councilman* is decided may cast doubt on the validity of that particular prosecution. We are concerned any amendment – including even “clarifying” amendments – may suggest to the courts that the statute must have a different meaning post-amendment than we believe it does currently, even though we think the statute currently strikes the appropriate balance. This inference may affect more than this one case, as the validity of any title III prosecution for the past interception of computer network communications could be clouded similarly. Thus, we believe such amendments could be potentially harmful to our common goal.

Moreover, if interpreted too broadly, an amendment could upset the framework which governs the balance between law enforcement and privacy in the e-mail context. For example, one such proposal would amend the meaning of “intercept”, by inserting “contemporaneous with transit” into the definition. If this amendment were to pass now, a court might interpret it to apply to title III and the acquisition of stored, unretrieved e-mail messages – a broad conclusion that would seriously impede countless criminal investigations while going well beyond that needed to reverse the panel’s result in *Councilman*.

Currently, under the Electronic Communications Privacy Act, law enforcement agencies may compel the disclosure of unretrieved e-mail in a customer’s inbox under 18 U.S.C. § 2703(a), using a warrant based upon probable cause. But under the broader interpretation of “contemporaneous with transit,” a title III order would be required. A broad interpretation would go well beyond merely reversing the First Circuit’s vacated decision in *Councilman*, but also the settled interpretation of stored e-mail from *Steve Jackson Games, Inc. v. United States Secret Service*, F.3d 457, 461 (5th Cir. 1994).

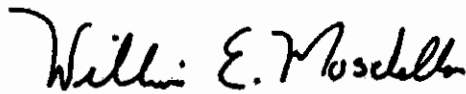
This broad construction also would effectively nullify section 209 of the USA PATRIOT Act. That section reflected Congress’ assessment that communications (in particular, voice communications) in electronic storage deserve somewhat less privacy protection than messages acquired in transit. Accordingly, section 209 allowed the former to be obtained by law enforcement with a warrant instead of a wiretap order. A broad reading of an amendment would thus effectively erase section 209 from the Act, and thereby place on law enforcement onerous demands that Congress previously had sought to ease.

It is generally accepted that when a law enforcement acquisition is limited only to those communications that already have occurred, a search warrant is the proper authority. But to acquire the content of communications that have yet to take place, the proper authority is a court order or other authority under title III. We believe this dichotomy has balanced well the privacy of communications on the one hand and the needs of law enforcement to fight crime on the other. Any amendments may disrupt the balance.

The Honorable F. James Sensenbrenner, Jr.  
Page 3

Thank you for the opportunity to present our views. Please do not hesitate to call upon us if we may be of additional assistance. The Office of Management and Budget has advised us that from the perspective of the Administration's program, there is no objection to this letter.

Sincerely,

A handwritten signature in black ink, reading "William E. Moschella". The signature is written in a cursive style with a large initial "W" and a stylized "M".

William E. Moschella  
Assistant Attorney General



**U.S. Department of Justice  
Office of Legislative Affairs**

Office of the Assistant Attorney General

*Washington, D.C. 20530*

July 12, 2005

The Honorable F. James Sensenbrenner, Jr.  
Chairman  
Committee on the Judiciary  
U.S. House of Representatives  
Washington, D.C. 20515

Dear Mr. Chairman:

This responds to your letter dated July 1, 2005, requesting the views of the Department of Justice (Department) regarding HR 1502, the Civil Liberties Restoration Act. The Department strongly opposes this bill and urges the Committee to take no action on it. If, however, the Committee believes it is appropriate to move this legislation, we request the opportunity to meet with you in advance of any action.

If enacted, the bill would seriously undermine homeland security, reduce the Government's ability to respond effectively to terrorism, virtually eliminate the Attorney General's control over immigration policy, provide additional incentives for illegal immigration, and abrogate aliens' rights to privacy. HR 1502 is also troubling because it imposes inappropriate and unworkable requirements, impairs the current procedures for protecting the public and avoiding the absconding of aliens during the pendency of removal proceedings against them, statutorily modifies certain practices that no longer exist and that have been addressed through less-damaging means, and undermines the ability of the Attorney General to interpret and administer the law in light of current circumstances, including national security and foreign policy concerns. Finally, HR 1502 would abolish and reorganize the Executive Office for Immigration Review (EOIR) and in the process terminate recent internal reforms that have permitted EOIR to adjudicate cases more fairly and efficiently.

Set forth below is a section by section analysis.

**Section 101 Limitation on Closed Immigration Hearings.** This section would sharply limit the closure of immigration hearings, even when an alien's privacy is at stake, and even in times of a national security crisis. Indeed, the bill permits closure only on a case-by-case basis, only when an immigration judge approves, and only when the Government can show that closure "is necessitated by a compelling governmental interest and is narrowly tailored to serve that interest." We oppose this provision.

The Honorable F. James Sensenbrenner, Jr.

As an initial matter, it is important to emphasize that the vast majority of closed removal cases are closed for the benefit of the alien, not the public interest. For example, hearings are typically closed when an alien is applying for asylum or when a spouse is testifying about domestic abuse. In addition, hearings are always closed in cases involving child abuse. The reason for closure is to protect the alien's privacy and to provide the alien greater comfort when testifying about the alleged abuses in his or her home country. Despite this weighty interest, Section 101 would restrict closure to only those individual cases in which the Government could prove that closure is necessary to advance a compelling Government interest and is narrowly tailored to serve that interest. Because an alien's privacy is often not a compelling *government* interest, and because the bill's strict scrutiny test is an exacting standard, aliens' privacy could very well be sacrificed. For this reason alone, the Department has serious concerns about the provision.

Moreover, section 101 needlessly undermines national security. As the Federal Bureau of Investigation (FBI) determined at the outset of the 9-11 investigation, closed proceedings for special interest aliens are essential to prevent sophisticated terrorist organizations, such as al Qaeda, from learning about the course and extent of the investigation. Further, the public disclosure of such information could cause terrorists to escape detection, alter their attack plans, obstruct pending proceedings, or deter detainees from cooperating with the ongoing investigation.

It is the considered judgment of the Government officials in charge of the terrorism investigation that, in the aftermath of 9-11, our national security could not be adequately safeguarded by allowing immigration judges to close hearings on a case-by-case basis. Such a system would have risked disclosure of the identities of aliens in special interest cases, and the Attorney General has determined that the identities of special interest aliens are sensitive precisely because their disclosure could allow terrorist organizations to discern patterns in the ongoing investigations and to react accordingly. On that point, the D.C. Circuit agreed with the Attorney General and therefore held that this list of names was exempt from disclosure under the Freedom of Information Act. See *Center for National Security Studies v. DOJ*, 331 F.3d 918 (D.C. Cir. 2003). Additionally, case-by-case closure would have compromised the confidentiality of cooperating aliens or witnesses, since observers would be able to discern from the failure of an alien or witness to oppose closure that he was cooperating with the Government.

Furthermore, as the FBI has explained, case-by-case closure would not have adequately protected information that may have appeared innocuous in isolation, but could have fit into a bigger picture by terrorist groups in order to thwart the Government's efforts to investigate and prevent terrorism. An immigration judge is simply not situated to see the overall pattern of the Government's investigation from the small segment that might be manifest in a particular case. As the Supreme Court has warned, judges are not sufficiently "familiar with 'the whole picture'" to second-guess Executive Branch determinations about whether the release of such information could assist enemy intelligence, and thereby harm the national security. *CIA v. Sims*, 471 U.S. 159, 178 (1985) ("What may seem trivial to the uninformed, may appear of great moment to one

The Honorable F. James Sensenbrenner, Jr.

who has a broad view of the scene and may put the questioned item of information in its proper context.” (citation omitted)). Thus, although Section 101, as drafted, would authorize partial closure of a hearing to protect classified information or the identity of a confidential informant, broader security measures may be necessary in the event of a national emergency, especially at the outset of the Government’s investigation, when information available to the investigators is piecemeal and its reliability is uncertain.

These national security concerns would be particularly severe if section 204 of the bill (discussed below) were passed as well. That provision transfers the immigration judges to an independent regulatory agency. Thus, critical national security decisions would be made, not by the Attorney General, his designees, or any other public official accountable to the American public, but by an independent regulatory agent, who might have an imperfect understanding of the national security consequences of open hearings.

Moreover, case-by-case closure would also impose difficult problems of administration. Should immigration judges decide to close individual cases or hearings, members of the press would likely challenge those determinations, and the adjudication of those challenges would itself be rife with potential for revealing critical information to terrorist organizations. In addition, a requirement of case-by-case (or hearing-by-hearing) justification for closure -- with the attendant prospect of press challenges and interlocutory judicial intervention -- would seriously disrupt removal proceedings and divert personnel and resources from the conduct of the ongoing terrorism investigations and the removal proceedings themselves.

It has been suggested that the Department’s concerns regarding section 101 are invalid in light of the fact that immigration judges can hold a closed “pre-hearing” to decide whether the actual hearing should be closed. The suggestion is incorrect. Although a closed pre-hearing could avoid some of the pitfalls of an open pre-hearing (such as disclosing, in the course of the pre-hearing, the very information the Government is attempting to protect), the closed pre-hearing does not avoid other serious national security concerns that underlie the Department’s opposition to the bill. First, as explained above, no single immigration judge is sufficiently familiar with the whole national security picture to assess whether the discrete information in a single case needs to be protected from disclosure. Such information may appear innocuous in isolation but could fit into a bigger picture that terrorist groups could use to thwart the Government’s efforts to investigate and prevent terrorism. Additionally, immigration judges may lack the expertise in national security affairs to render a determination that adequately protects the American people from harm. Clearly, it makes more sense for critical national security decisions to be made by those with the most knowledge and experience in national security affairs. Finally, case-by-case closure would also create the problems of administration explained above. In any event, section 101 plainly prohibits closed pre-hearings. Under the draft bill, no “portion[]” of a removal proceeding can be closed to the public unless the government satisfies the exacting strict scrutiny standard. Thus, the bill provides no effective mechanism for shielding sensitive information from disclosure.

The Honorable F. James Sensenbrenner, Jr.

Five points are important to bear in mind regarding the Government's handling of the closure process to date. First, the closed immigration hearings were not "secret" proceedings that prevented an alien from retaining counsel, notifying friends or family, and discussing his case in public. Second, closure of proceedings did not affect an alien's due process protections, which as the Third Circuit has explained are extensive in this context. *North Jersey Media Group, Inc. v. Ashcroft*, 308 F.3d 198 (3d Cir. 2002). Third, the Department has not closed any immigration proceeding pursuant to the special procedures for over two and half years. This fact underscores that such procedures, although critical in times of emergency have been used only sparingly. Fourth, the procedures withstood constitutional attack in *North Jersey Media Group, Inc.* which flatly rejected the notion that the public has a First Amendment right of access to sensitive immigration proceedings. Although the Sixth Circuit reached a contrary conclusion in *Detroit Free Press v. Ashcroft*, 303 F.3d 681 (6th Cir. 2002), we do not agree that there is any basis for inferring that the public has a constitutional right to attend hearings before the immigration judges. Fifth, the need for confidentiality is underscored by Congress's own decision to bar public access to its own investigation of past and possible future terrorist attacks. See S. Schmidt & K. Khan, "Lawmakers Question CIA on Dirty-Bomb Suspect," Washington Post A11 (June 13, 2002); D. Priest & J. Eilperin, "'We Should Have' Known, Goss Says of 9/11," Washington Post A12 (June 12, 2002). All of these factors counsel against enactment of this provision.

Finally, this provision raises a serious constitutional concern as it may infringe upon the President's authority to control and protect national security information. See, e.g., *Dep't of the Navy v. Egan*, 484 U.S. 518, 527 (1988) ("The President . . . is the 'Commander in Chief of the Army and Navy of the United States.' His authority to classify and control access to information bearing on national security . . . flows primarily from this constitutional investment of power in the President and exists quite apart from any explicit congressional grant.") (citations omitted).

**Section 201 Timely Service Of Notice.** This provision would require the Department of Homeland Security (DHS) to serve a notice to appear on every alien arrested or detained under the Immigration and Nationality Act (INA) within 48 hours. In addition, the bill provides that every alien detained for more than 48 hours must be brought before an immigration judge within 72 hours of arrest. The only exception to the foregoing requirements is for aliens who are certified under the special terrorism detention provisions in section 236A(a)(3) of the INA.

The Department defers to DHS regarding the impact of the 48-hour provision. We note, however, that under current regulations, DHS is already required to make decisions on the issuance of charging documents and whether to detain the alien in connection with those proceedings within 48 hours, except in exceptional circumstances. All the bill would do in this regard is eliminate the exception for exceptional circumstances, thereby tying the Government's hands in the event of a national crisis. Further, the Department opposes the requirement to bring every alien, if not immediately released, before an immigration judge within 72 hours of arrest. This provision would substantially undermine the provisions of current law relating to the detention of aliens during the pendency of removal proceedings, would encourage hasty decision



The Honorable F. James Sensenbrenner, Jr.

making in a national emergency, and would impose unworkable burdens on the immigration process itself. Indeed, last year, the immigration judges conducted over 33,000 custody hearings. By imposing a stringent time limitation, the 72-hour requirement would create an onerous burden for immigration judges and would disrupt their ability to handle the many other important issues arising in the approximately 300,000 cases they handle each year.

These new provisions essentially would import into immigration proceedings the legal requirements similar to those applicable to pre-trial detention of individuals charged with criminal offenses. But the ability of the Government to detain aliens during the pendency of removal proceedings is well established and is quite unlike the legal principles applicable to criminal defendants. Indeed, as the Supreme Court has determined, aliens have no legal right to be released on bond during the pendency of removal proceedings. The Court has repeatedly “recognized detention during deportation proceedings as a constitutionally valid aspect of the deportation process,” *Demore v. Kim*, 538 U.S. 510 (2003), and has acknowledged that “Congress eliminated any presumption of release pending deportation, committing that determination to the discretion of the Attorney General.” *Reno v. Flores*, 507 U.S. 292, 306 (1993); *see also Carlson v. Landon*, 342 U.S. 524, 534 (1952); *Reno v. Flores*, 507 U.S. at 295 (“Congress has given the Attorney General broad discretion to determine whether, and on what terms, an alien arrested on suspicion of being deportable should be released pending the deportation hearing”). Accordingly, there is no justification for adopting section 201.

**Section 202 Individualized Bond Determinations.** This provision would generally require the government to release an alien from detention unless the adjudicator makes an individualized determination “that the alien poses a danger to the safety of other persons or is unlikely to appear for future proceedings.” Remarkably, the bill permits the adjudicator to consider only two factors, neither of which is national security or immigration policy.

The Department of Justice has serious concerns about Section 202 because the alien’s individual dangerousness and likelihood of flight are not the only factors to take into account in determining whether the alien should be detained during the pendency of removal proceedings. A recent decision arising in connection with aliens arriving illegally by sea made clear why the immigration judges and the Board of Immigration Appeals (BIA) also need to consider, in addition to dangerousness and flight risk, other factors relating to national security and immigration policy in making bond determinations. *Matter of D-J-*, 23 I. & N. Dec. 572 (A.G. 2003). In that case, immigration officials offered evidence to the Attorney General of two broad areas of national security that were implicated by the order releasing D-J- and others like him. First, they demonstrated that release of D-J- and others who arrived on his vessel would “tend to encourage further surges of mass migration from Haiti by sea, with attendant strains on national and homeland security resources” that could be “used in supporting operations elsewhere.” Moreover, further mass migration “place[d] the lives of aliens at risk.” Second, they showed that, “in light of the terrorist attacks of September 11, 2001, there is [an] increased necessity in preventing undocumented aliens from entering the country without the screening of the immigration inspections process” because “third country nation[al]s” were using the countries

The Honorable F. James Sensenbrenner, Jr.

such as “Haiti as a staging point for attempted migration to the United States.” The Attorney General agreed with the INS and reversed the decision of the BIA, concluding that national security and immigration policy concerns were appropriate considerations in bond determinations. Section 202 could be interpreted to effectively overrule the Attorney General’s judgment that immigration judges should not ignore national security considerations. Indeed, the bill could be interpreted to legally preclude judges from taking these considerations into account.

Moreover, the bill would be a radical break with precedent and tradition for immigration detention by creating a right for aliens to be released from custody unless the Government makes an affirmative finding relating to danger to the community or risk of flight. Nowhere does the INA grant aliens any right to be released on bond – let alone a right to be released even when there are national security reasons to detain. Instead the statute gives the Attorney General the broad discretion to grant bond *if* he concludes bond is merited. Moreover, the use of “reasonable presumptions and generic rules” in immigration custody matters has been upheld by the Supreme Court. *Flores*, 507 U.S. at 313-14 (detention was based “upon a ‘blanket’ presumption of the unsuitability of custodians other than parents, close relatives, and guardians,”); *Carlson v. Landon*, 342 U.S. 524, 541-42 (1952). Finally, it is important to note that, under current law, similarly situated aliens, receive individualized determinations. See, e.g., *Matter of D-J-*, 23 I. & N. Dec. at 583 (“I have given full consideration to the *individual aspects of respondent's claim* for bond based on the record in this proceeding. I find nothing in respondent's individual case that warrants granting him release on bond when balanced against the above-described compelling factors that militate against such release in the case of undocumented aliens attempting illegal entry into the United States under the circumstances presented by the October 29 influx.”) (emphasis added).

Finally, the bill could create additional problems by preventing DHS from taking an alien back into custody, based on a change of circumstances, without a *prior* hearing before an immigration judge. The ability to return the alien to custody would be illusory in the great majority of cases because, as soon as DHS notified the alien of the upcoming hearing, most aliens would simply choose to abscond. Even worse, the bill expressly provides that an order of removal is not a changed circumstance warranting a return to custody. This provision simply turns a blind eye to reality. As DHS has found, a large majority of non-detained aliens who are found to be removable will flee. Instead, Congress should retain the practice under current law, as reaffirmed by the Board over the years, that DHS is able to take an alien back into custody after any change in circumstances, including the entry of a removal order, subject to a subsequent review by the immigration judge.

**Section 203 Limitation On Stay Of A Bond.** This section would limit DHS’s ability to challenge an immigration judge’s decision to release an alien who presents a flight risk or a danger to the community. Under the bill, an immigration judge’s decision to release an alien could be stayed by the Board of Immigration Appeals (BIA) for no more than 30 days and only if the Government could demonstrate, among other things, irreparable harm from the denial of a stay and a likelihood of success on the merits. In effect, the bill would render invalid the

The Honorable F. James Sensenbrenner, Jr.

Attorney General's sensible regulation providing for a short-term "automatic stay" of an immigration judge's decision to release an alien pending appeal of that decision to the BIA. See 8 CFR 1003.19(i)(2).

The Department opposes section 203 because the "automatic stay" regulation promotes an orderly process for reconciling conflicting Executive Branch decisions, and it balances the Government's interests in public safety and minimizing flight risk with the aliens' interest in securing their release. The conflict within the Executive Branch arises from the fact that both the Attorney General and the Secretary of Homeland Security concurrently possess the authority to release under section 236(a). In some cases, DHS and the Attorney General's initial designee, an immigration judge, may disagree on whether to release an alien. Under current law, this disagreement is resolved by the BIA (whose members are also designees of the Attorney General). The purpose of the automatic stay is to maintain the status quo long enough to allow the BIA enough time to resolve the dispute in a reasoned manner.

Indeed, the regulation was originally promulgated because, as the Attorney General determined, "[a] custody decision that allows for immediate release is effectively final if, as the [DHS] appeal would necessarily assert, the alien turns out to be a serious flight risk or a danger to the community." See 63 Fed. Reg. 27441, 27447 (May 19, 1998); see also *Demore*, 538 U.S. at 523 (2003) ("deportation proceedings would be vain if those accused could not be held in custody pending the inquiry into their true character") (internal quotations omitted). Without the automatic stay, an alien could have absconded, or could have committed multiple crimes, by the time the BIA reviews the record and decides whether DHS or the immigration judge was correct. Moreover, these concerns are not merely theoretical; it is well known that high absconding rates have long plagued the immigration system. See *id.* at 528. In just the last five fiscal years, for example, almost 62,000 aliens (45%) who were released from custody during the pendency of their removal hearings failed to appear for their scheduled removal hearings. EOIR, *FY 2004 Statistical Year Book*, at H3 (March 2005).

Under the emergency-stay-motion procedures that existed prior to the automatic stay regulation, a "significant window of time" was created "wherein the alien may be released while" a complete record of proceedings and the parties' briefs were prepared and transmitted to the BIA in Falls Church, Virginia, and the BIA reviewed the record and adjudicated the motion. To avoid unmerited release during that window of time, the BIA would have had to make on-the-spot determinations in each case as to whether a stay pending appeal should be granted. To make matters worse, the BIA's nationwide jurisdiction (which includes Hawaii and Guam) meant that, "due to the time difference between the east and west coast, an alien may be ordered released after the Board has closed for the day." 66 Fed. Reg. at 54909, 54910-54911 (Oct. 31, 2001).

Further, it is important to note that the automatic stay regulation has been invoked only in relatively serious cases and only for a reasonable duration. Although immigration judges conduct approximately 30,000 custody hearings every year, EOIR, *FY 2004 Statistical Year*

The Honorable F. James Sensenbrenner, Jr.

*Book*, at B5, there have only been a few hundred cases in which DHS has invoked the automatic stay, in total, during the nearly four years since the interim rule was promulgated in October 2001. As such, the automatic stay is a sparingly used but important public safeguard against the unwarranted release of aliens who otherwise would be adjudicated by the BIA to be a serious flight risk or a danger to the community. Without the automatic stay, DHS's right to appeal in these cases would be negated as a practical matter.

**Section 204 Immigration Review Commission.** This section is one of the most problematic and ill-advised provisions in the bill. Inconsistent with longstanding immigration law and the U.S. Constitution, it would virtually eliminate the Attorney General's control over immigration policy and transfer that power to an independent agency. Specifically, the bill would abolish EOIR and replace it with "an independent regulatory agency" within the Department called the Immigration Review Commission (IRC). This section would also provide that: (1) the Director of the IRC would be appointed by the President and confirmed by the Senate; (2) the BIA would become the Board of Immigration Review (BIR) and its composition would be a chair and not less than 14 other immigration appeals judges appointed by President; (3) BIR would review immigration judge orders de novo; (4) the BIR would be required to decide cases in 3 member panels and would be authorized to affirm without opinion only if it adopts the immigration judge's findings and conclusions in total; (5) immigration judges would be appointed by the Director for a 12 year term; and (6) immigration judges and immigration appeals judges could be removed only for cause.

The Department strongly opposes this section, which would remove ultimate administrative authority from the Attorney General. First, making EOIR an "independent regulatory agency" runs counter to the well-established principle that the exercise of immigration authority is a political and foreign policy matter for the Executive Branch. *Shaughnessy v. Mezei*, 345 U.S. 206, 210 (1953). As the Supreme Court has explained, "the power to expel or exclude aliens" is "a fundamental sovereign attribute". *Id.* It is inextricably intertwined with national security, foreign policy, and the identity of the nation. See *INS v. Aguirre-Aguirre*, 526 U.S. 415, 425 (1999) ("we have recognized that judicial deference to the Executive Branch is especially appropriate in the immigration context where officials 'exercise especially sensitive political functions that implicate questions of foreign relations.'" (citation omitted)); *Landon v. Plasencia*, 459 U.S. 21, 34 (1982) ("it must weigh heavily in the balance that control over matters of immigration is a sovereign prerogative, largely within the control of the executive and the legislature."); *Hampton v. Mow Sun Wong*, 426 U.S. 88, 101 n.21 (1976) ("the power over aliens is of a political character and therefore subject only to narrow judicial review."); see also 8 U.S.C. 1103(g). Like Congress, the Executive Branch has plenary power to address immigration issues. The Supreme Court has stated that the "exclusion of aliens" stems "not alone from legislative power but is inherent in the executive power to control the foreign affairs of the nation." *Knauff v. Shaughnessy*, 338 U.S. 537, 542 (1950). "[A]ll executive power (other than purely ministerial authority) must ultimately be subject to Presidential control." *Secretary of Education Review of Administrative Law Judge Decisions*, 15 Op. O.L.C. 8, 14 (1991). Thus, it is unconstitutional and inappropriate for Congress to hand over the keys to our borders to an

The Honorable F. James Sensenbrenner, Jr.

independent agency. The only way to ensure that the interpretation of our immigration laws will be consistent with foreign policy and other basic principles of sovereignty is to ensure that the Executive Branch has the ability to enforce and interpret the federal immigration statutes, subject to limited and deferential judicial review. Making EOIR an “independent regulatory agency” would effectively end the Executive Branch control and accountability for this aspect of foreign policy and national security.

Second, section 204 would eviscerate several of the important immigration reforms that the Department and EOIR have developed in order to make the adjudication of immigration cases efficient, prompt, and fair. The Department and EOIR have enhanced the efficiency of EOIR’s adjudications (and thereby reduced a substantial backlog of cases) by affording immigration judges, who are the actual factfinders, appropriate deference in the administrative appellate review process. In addition, and consistent with this principle, the BIA instituted a process whereby it could summarily affirm an immigration judge’s decision through a single Board member review process. This practice, which was first implemented in 1999 and is commonly referred to as “streamlining,” is a careful process that has assisted EOIR in managing its cases fairly and efficiently. Indeed, every court of appeals that considered the Board’s “streamlining” process has upheld it. E.g., *Falcon Carriche v. Ashcroft*, 350 F.3d 845 (9<sup>th</sup> Cir. 2003); *Georgis v. Ashcroft*, 328 F.3d 962, 967 (7<sup>th</sup> Cir. 2003); *Mendoza v. United States Att’y Gen.*, 327 F.3d 1283, 1288 (11<sup>th</sup> Cir. 2003); *Soadjede v. Ashcroft*, 324 F.3d 830 (5<sup>th</sup> Cir. 2003). The courts of appeals regularly use “summary affirmance” orders themselves, in the immigration context and in other contexts as well, to resolve fact-bound cases that do not raise serious legal issues. In essence EOIR would revert back to an agency that would have tremendous backlogs, insurmountable delays, and no possible prospects for resolving cases quickly. As a result EOIR would not be able to order illegal aliens removed (or grant relief from removal) promptly. Detained aliens would be detained longer, and non-detained aliens would be given additional opportunities to flee, increasing the population of illegal aliens in this country. Insubstantial cases would crowd out consideration of substantial cases, and the only beneficiaries would be aliens pursuing meritless cases for the sole purpose of delay.

Finally, section 204 raises other constitutional concerns. Section 204 would unconstitutionally remove existing federal officers within the EOIR by abolishing their offices, reconstituting those offices by statute (sometimes under a different name), and requiring the appointment of new officers. Congress lacks the authority to remove officers of the Executive Branch except through impeachment and conviction or through *bona fide* abolition of their office. See *Myers v. United States*, 272 U.S. 52, 122 (1926). Likewise section 204 would run afoul of the Appointments Clause of the Constitution and create serious separation of powers problems. For all these reasons, Congress should reject section 204.

**Section 301 Termination Of The NSEERS Program; Establishment Of Reasonable Penalties For Failure To Register.** This section would terminate the National Security Entry-Exit Registration System (NSEERS) a program that is administered by DHS. In addition, it would require the administrative closure of removal cases brought “solely for failure to comply

The Honorable F. James Sensenbrenner, Jr.

with the requirements of the NSEERS program” or aliens placed in removal proceedings as a result of NSEERS and who were eligible for an immigration benefit (or had an application pending before Department of Labor or DHS and a visa available).

The NSEERS program was commenced by the former Immigration and Naturalization Service (INS). When INS was abolished and DHS created, NSEERS became a program administered by DHS. Accordingly, the Department defers to DHS regarding this provision. Nevertheless, the Department believes that NSEERS has had a beneficial impact on the fight against terrorism in the aftermath of September 11, 2001. NSEERS, coupled with all of the other efforts DHS, Department of State, and DOJ have made to tighten border security and enhance consular screening undoubtedly have made it more difficult for terrorists to enter the United States. The abolition of a program that terrorists know is designed to thwart their entry into the United States would send the wrong message about this country’s preparedness. The Department is opposed to the abolition of NSEERS.

**Section 302 Exercise of Prosecutorial Discretion.** This section would compel the Secretary to exercise prosecutorial discretion in deciding whether to exercise its enforcement powers against an alien. The section sets forth a list of factors that the Secretary “shall” take into account when deciding whether to exercise prosecutorial discretion.

The Department defers to DHS regarding this provision. However, the Department has serious concerns about the constitutionality of section 302 as Congressional intrusions into the Executive Branch’s exercise of prosecutorial discretion are improper. *See Reno v. American-Arab Anti-Discrimination Comm.*, 525 U.S. 471, 489 (1999) (prosecutorial discretion is “a special province of the Executive”); *Heckler v. Chaney*, 470 U.S. 821, 832 (1985) (prosecutorial decision “has long been regarded as the special province of the Executive Branch”); *Prosecution for Contempt of Congress of an Executive Branch Official Who Has Asserted a Claim of Executive Privilege*, 8 Op. O.L.C. 101, 125 (1984) (“[T]he constitutionally prescribed separation of powers requires that the Executive retain discretion with respect to whom it will prosecute for violations of the law.”). The Department also has significant concerns about the litigation that Section 302 would create if enacted. It is possible that courts could construe Section 302 so that an alien could challenge the decision not to exercise prosecutorial discretion. Because DHS already has prosecutorial discretion (and exercises that authority in appropriate cases), it does not appear that this statutory provision would enhance that authority at all and would more likely produce needless litigation over the scope and meaning of the provision.

**Section 303 Civil Penalties For Technical Violations Of Registration Requirements.** This section revises Section 266 of the INA which is a penalty provision administered by DHS. The Department defers to DHS regarding its view of this provision. However, the Department has concerns that it reduces the penalties for failure to comply with registration requirements, including the elimination of criminal misdemeanor offense.

The Honorable F. James Sensenbrenner, Jr.

**Section 304 NCIC Compliance With The Privacy Act.** This section would require that data entered into NCIC must meet the accuracy requirements of the Privacy Act. The Privacy Act governs the collection, maintenance and use of information about individuals. The Act authorizes federal agencies to "exempt" their records systems from certain requirements of the Act. These exemptions reflect Congress' express recognition that special treatment may be required for law enforcement records. Specifically, paragraph (j)(2) of the Act permits the head of any agency to promulgate rules to exempt any system of records within the agency from any part of the Act [except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i)]. In addition, when an agency claims an exemption, it must publish reasons for the exemption in the Federal Register and afford the public an opportunity to comment. In accordance with paragraph (j)(2) of the Act, on January 31, 2003, the FBI published a proposed rule in the Federal Register exempting NCIC from paragraph (e)(5) of the Act which requires federal agencies to maintain records "with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." See 68 Federal Register 4974 (January 31, 2003). No comments were received regarding the proposed rule. Accordingly, after the close of the public comment period, on March 24, 2003, the FBI published a final rule exempting NCIC from paragraph (e)(5) of the Act. See 68 Federal Register 14141 (March 24, 2003).

The justification for the exemption from paragraph (e)(5) is because in the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. Furthermore, the restrictions imposed by paragraph (e)(5) would limit the ability of trained investigators to exercise their judgment in reporting on investigative developments necessary for effective law enforcement. Additionally, the vast majority of records in NCIC come from other federal, state, local, joint, foreign, tribal, and international agencies and, therefore, it is administratively impossible to guarantee that the records comply with this provision. See 68 Federal Register 14141 (March 24, 2003).

There are quality assurance procedures in place for NCIC that provide a robust mechanism to ensure the accuracy of records over time and to limit the risk of misidentification or false arrests. The FBI's Criminal Justice Information Services (CJIS) Division requires Control Terminal Agencies (CTAs) for each state and federal service seeking access to NCIC to enter into a User Agreement that outlines certain responsibilities to maintain the integrity of the system. The CTAs enter into separate agreements with local agencies that require all users to follow applicable rules to access and use NCIC. Section 3 of the NCIC 2000 Operating Manual includes standards for security and audits for NCIC CTAs. The security provisions provide guidance for CTAs, including personnel, physical and technical security, as well as user authorization and dissemination. Furthermore, all federal and state CTAs are required to conduct biennial audits to ensure compliance with state and CJIS' policy and regulations.



The Honorable F. James Sensenbrenner, Jr.

In addition, at least once every two years CJIS conducts random audits of a sample of criminal justice agencies for the Wanted Persons, Missing Persons, Vehicles and Protection Order files in NCIC. The audits include reviews of: (1) accuracy -- CTAs should maintain necessary documentation as required by CJIS policy; (2) completeness -- information should be comprised of all pertinent available information; (3) timeliness -- entry, modification, update and removal of information should be completed as soon as possible after information is available; (4) security -- an organization should protect its information from unauthorized access; and (5) dissemination -- in accordance with applicable laws and regulations.

Moreover, NCIC has quality control and validation procedures which include: (1) automatic computer edits which reject certain types of errors in data; (2) automatic purging of records after they are in a file for a prescribed period of time; (3) periodic quality control checks by the FBI's CJIS Data Integrity Staff where errors are classified as serious or non-serious and are followed by appropriate action by CJIS; and (4) periodically furnishing lists of all records on file for validation by agencies. Quality Control measures include procedures where the accuracy of a record must be double checked by a second party and verified utilizing all available cross checks. The NCIC 2000 manual explains the requirements of "timely entry" for NCIC 2000 files and explains that records should be complete and include all information available on a person or property at the time of entry. Furthermore, the originating agency is responsible for confirming that the record is complete, accurate, and still outstanding or active, which should include a review of whether additional information is missing from the original record that could be added.

In sum, the FBI has only claimed an exemption in accordance with the Privacy Act for the NCIC to the extent permissible pursuant to paragraph (j)(2) of the Act. The exemption has not changed the quality assurance measures for entry, audit, validation and hit confirmation that are already in place for NCIC records to ensure the accuracy of records and to limit the risk of misidentification and false arrests. For all these reasons, therefore, the Department opposes section 304.

**Section 401 Modification Of Authorities On Review Of Motions To Discover Materials Under Foreign Intelligence Surveillance Act Of 1978.** Section 401 would provide a strong presumption in favor of the disclosure of highly sensitive or classified materials, amending the FISA search, surveillance, pen register, and business records provisions. When Congress enacted FISA in 1978, it recognized that the information involved in national security investigations must be safeguarded; therefore it provided statutory protections for that information in FISA itself. For example, a court reviewing a FISA surveillance or search to determine whether it was lawfully authorized and conducted shall review the FISA application, order and related materials in camera and ex parte upon sworn affidavit from the Attorney General that disclosure or an adversary hearing would harm the national security of the United States. Moreover, when determining whether the search of surveillance was lawfully authorized and conducted, disclosure to an aggrieved person can be made "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance" or search.



The Honorable F. James Sensenbrenner, Jr.

Section 401 would turn this statutory scheme on its head, presumptively requiring disclosure of some of our most sensitive national security information. Specifically, section 401(a) and (b) would *require* disclosure of portions of the FISA search and surveillance applications, orders, and related materials to either an “aggrieved person” and/or his or her counsel “unless the court finds that such disclosure would not assist in determining *any* legal or factual issue *pertinent* to the case.” (Emphasis added). It is hard to imagine a circumstance in which information sought would not “assist” the court in determining “any” legal or factual issue “pertinent” to the case.

The amendments in section 401(c) to section 405 of FISA, which addresses pen register and trap and trace devices, are potentially even more problematic. Pen registers and trap and trace devices are minimally invasive investigative tools. And existing law, which requires pen registers and trap and trace devices to be authorized by a judge, already provides more protection than is constitutionally required, as the Supreme Court has held that no court approval is constitutionally necessary to install or use a pen register or trap and trace device. *Smith v. Maryland*, 442 U.S. 735, 744 (1979). Section 401 would require disclosure not only of portions of the application, order, or other materials relating to the use of such a device, but also “evidence or information obtained or derived from the use” of such a device. This implicates potentially all information related to a given investigation, if it is merely “derived” from the use of a pen register or trap and trace device.

Finally, section 401(d) appears to be an attempt to impose the same presumption of disclosure with respect to information obtained pursuant to the FISA business records authority. For the reasons set forth above, we would oppose any presumption in favor of disclosing this sensitive national security information. Moreover, as it is written, section 401(d) would appear to apply to *all* disclosures of FISA business records information, which would include disclosures to other governmental agencies. This amendment would therefore have a strong deterrent effect on information-sharing, which the Department must oppose. As witness after witness recently testified before House and Senate Committees, our ability to share information has been critical to our ongoing efforts to protect Americans and the values we cherish.

To put the matter simply, section 401 would place investigators in the position of forgoing the use of critical investigatory tools for fear of jeopardizing sensitive national security information. Suppose, for example, the information underlying an application to the FISA Court came from a foreign Government; if the foreign Government knows that United States law contains a presumption of disclosure of this information to a petitioner (or a criminal defendant), the foreign Government could decide not to share the information or to place restrictions on the use of the information. A dilemma would also arise if the source of the information in the application were a sensitive human source who could be endangered through disclosure, leaving investigators with the choice of endangering the source or not obtaining the FISA Court order. The presumption in favor of disclosure in litigation would inevitably have a negative impact on our ability to gather information about, and eventually prosecute individuals for, serious international terrorism and espionage-related crimes.

The Honorable F. James Sensenbrenner, Jr.

**Section 402 Data-Mining Report.** Section 402 would require a detailed report to Congress each time an agency “use[s]” or “develop[s]” a “data-mining technology.” But section 402(a)(1) defines “data-mining” so ambiguously that it could be read to require reports to Congress for routine law enforcement procedures. “Data-mining” is defined as a query run on any database that “was obtained from or remains under the control of a non-Federal entity,” so long as the query “does not use a specific individual’s personal identifiers” and “is conduct[ed]” by a department or agency “to find a pattern indicating terrorist or other criminal activity.”

The Department believes that the definition used in the legislation is ambiguous in at least two important ways, at least one of which vitiates its apparent intent to single out pattern-based data-mining. First, “database” is defined to include all private databases and non-public state and local databases, as well as all non-public federal databases maintained “for purposes other than intelligence or law enforcement.” Although the legislation specifically excludes Internet sites and information available to the public without a fee, this definition would nonetheless include many databases useful for intelligence and law enforcement, such as some state DMV databases. Second, the definition of “data-mining” is also ambiguous because the term “specific individual’s personal identifiers” is undefined. It is unclear, for example, whether telephone numbers, license plate numbers, workplaces, and even cities of residence would constitute “personal identifiers.” Because section 402 requires a report to Congress when data-mining queries do not “use” these “specific personal identifiers,” the scope of the reporting obligation would be unclear. Consequently, many routine criminal and intelligence investigative procedures—such as determining who owns a car with a particular license plate, who owns a particular telephone number, or what computer corresponds with a particular IP address—could potentially constitute a “data-mining technology” that would require a report to Congress.

In addition, section 402(b)(2)(E) requires a “list and analysis of the laws and regulations that govern the information to be collected, reviewed, gathered, and analyzed with the data-mining technology.” This requirement is not limited to those “laws and regulations” that are actually relevant to the data-mining technology or to use of the information for law enforcement or intelligence purposes; rather, it includes *all* laws and regulations that govern the information in question.

Because many of the databases described in the section are not under federal control, in which case the federal government will have no way of knowing the universe of persons whose information is contained in those databases, and because in any event the entities who hold the relevant information may be under no legal obligation to provide the notice discussed, we believe that the concern apparently underlying this reporting requirement would be more effectively dealt with, if at all, through other means.

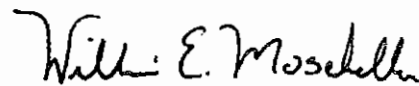
**Section 403 Privacy Protections on Government Access to Library, Bookseller, and Other Personal Records Under Foreign Intelligence Surveillance Act of 1978.** Section 403 would prevent the FISA Court from issuing an order under section 215 of the Patriot Act unless the Government provides “specific and articulable facts” giving “reason to believe that the

The Honorable F. James Sensenbrenner, Jr.

person to whom the records pertain is a foreign power or an agent of a foreign power.” Raising the standard to specific and articulable facts would make it more difficult to obtain records in a terrorism investigation than through a grand jury subpoena in an ordinary criminal investigation. This standard, which is significantly higher than the standard under which federal grand juries can subpoena records in ordinary criminal investigations, would disable the Government from using a section 215 order to develop evidence at the early stages of an investigation, which is precisely when such an order is the most useful. Section 403, with this higher standard, would disallow investigators from acquiring records that were relevant to an ongoing international terrorism or espionage investigation.

Suppose, for example, investigators are tracking a known al Qaeda operative and see him having dinner with three people, who split the check four ways and pay with credit cards. Investigators know nothing about the other individuals except that they had dinner with an al Qaeda operative, which would not constitute specific and articulable facts that each and every one of them is a terrorist. As an investigative matter, however, a responsible agent conducting an investigation would want to know who those individuals are. To do so, the agent could seek court approval for a section 215 order for the credit card slips from the restaurant. While investigators could demonstrate that this information is relevant to the ongoing investigation (and thus meet the existing standard under section 215), they could not demonstrate sufficient specific and articulable facts that those individuals are agents of a foreign power, as section 403 would require. Raising the standard above relevance, and requiring specific and articulable facts giving “reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power,” thus would serve to deny terrorism and espionage investigators information that is relevant to their investigations.

Sincerely,

A handwritten signature in dark ink, appearing to read "William E. Moschella". The signature is fluid and cursive, with the first name "William" and last name "Moschella" clearly distinguishable.

William Moschella  
Assistant Attorney General