



governmentattic.org

"Rummaging in the government's attic"

Description of document: Copies of certain Department of Justice (DOJ) views letters from the 107th and the 108th Congresses, 2001-2005

Requested date: 24-December-2012

Released date: 10-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 10, 2013

Re: OLA/13-01336 (F)
VRB:DRH:ND

This responds to your Freedom of Information Act (FOIA) request dated December 24, 2012, and received in this Office on January 2, 2013, for copies of certain views letters from the 107th and 108th 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 six documents, totaling fifty pages, were located that are responsive to your request. I have determined these documents, which provide the Department's views on the Foreign Intelligence Surveillance Act of 1978, Violent Crime Control Law Enforcement Act of 1994, Sarbanes-Oxley Act of 2002, Help America Vote Act of 2002, Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, and Intelligence Reform and Terrorism Prevention Act of 2004, are appropriate for release without excision and copies are enclosed. 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", is located below the "Sincerely," text.

Vanessa R. Brinkmann
Counsel, Initial Request Staff

Enclosures



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

October 1, 2001

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

Dear Senator Graham:

I am writing to relay to you the views of the Department of Justice on the constitutionality of amending the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1800-1863 ("FISA"), so that a search may be approved when the collection of foreign intelligence is "a significant purpose" of the search. In its current form, FISA requires that "the purpose" of the search be for the collection of foreign intelligence. 50 U.S.C. § 1804(a)(7)(B) and 50 U.S.C. § 1823(a)(7)(B). We believe that this amendment would not violate the Fourth Amendment. Amending FISA merely gives the Department the flexibility to conduct foreign intelligence surveillance that is permitted by the Constitution itself.

I

The Fourth Amendment declares that, "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. Amend. IV (emphasis added). The Amendment also declares that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized." *Id.*

Thus, the touchstone for review is whether a search is "reasonable." See, e.g., *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 652 (1995) ("[a]s the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a government search is 'reasonableness.'"). When law enforcement undertakes a search to discover evidence of criminal wrongdoing, the

Supreme Court has said that reasonableness generally requires a judicial warrant. See *id.* at 653. But the Court has made clear that a warrant is not required for all government searches. A warrantless search can be constitutional "when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *Id.*

As a result, the Court properly has found a variety of warrantless government searches to be consistent with the Fourth Amendment. See, e.g., *Pennsylvania v. Labron*, 518 U.S. 938 (1996) (per curiam) (certain automobile searches); *Acton*, *supra* (drug testing of high school athletes); *Michigan v. Dept. of State Police v. Sitz*, 496 U.S. 444 (1990) (drunk driver checkpoints); *Skinner v. Railway Labor Executives' Assn.*, 489 U.S. 602 (1989) (drug testing of railroad personnel); *Treasury Employees v. Von Raab*, 489 U.S. 656 (1989) (random drug testing of federal customs officers); *United States v. Place*, 462 U.S. 696 (1983) (temporary seizure of baggage); *Michigan v. Summers*, 452 U.S. 692 (1981) (detention to prevent flight and to protect law enforcement officers); *Terry v. Ohio*, 392 U.S. 1 (1968) (temporary stop and limited search for weapons).

In these circumstances, the Court has examined several factors to determine whether a warrantless search is reasonable. As the Court stated just last Term: "When faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like, the Court has found that certain general, or individual, circumstances may render a warrantless search or seizure reasonable." *Illinois v. McArthur*, 121 S. Ct. 946, 949 (2001). In creating these exceptions to its warrant requirement, the Court has found that, under the totality of the circumstances, the "importance of the government's interests" has outweighed the "nature and the quality of the intrusion on the individual's Fourth Amendment interests." See *Tennessee v. Garner*, 471 U.S. 1, 8 (1985).

Of particular relevance here, the Court has found warrantless searches reasonable when there are "exigent circumstances," such as a potential threat to the safety of law enforcement officers or third parties. The Court has also recognized that a government official may not need to show the same kind of proof to a magistrate to obtain a warrant for a search unrelated to the investigation of a crime "as one must who would search for the fruits or instrumentalities of crime." *Camara v. Municipal Court of San Francisco*, 387 U.S. 523, 538 (1967). For example, "[w]here considerations of health and safety are involved, the facts that would justify an inference of 'probable cause' to make an inspection are clearly different from

those that would justify such an inference where a criminal investigation has been undertaken." *Id.* See also *Indianapolis v. Edmond*, 531 U.S. 32, 44 (2000) (in context of seizure and exigent circumstances, Fourth Amendment would permit appropriately tailored roadblock to thwart an imminent terrorist attack or catch a dangerous criminal who is likely to flee).

II

This analysis of Fourth Amendment doctrine demonstrates that the government may conduct searches to obtain foreign intelligence that do not meet the same standards that apply in the normal law enforcement context. It is important to understand the current shape of Fourth Amendment law, and how it would apply to the circumstances at hand, in order to evaluate the constitutionality of the proposed amendment to FISA.

As we have noted earlier, the Fourth Amendment's reasonableness test for searches generally calls for a balancing of the government's interest against the individual's Fourth Amendment interests. Here, the nature of the government interest is great. In the counter-intelligence field, the government is engaging in electronic surveillance in order to prevent foreign powers or their agents from obtaining information or conducting operations that would directly harm the security of the United States.

To be sure, the Supreme Court has subjected counter-intelligence searches of purely domestic terrorist groups to a warrant requirement. When it first applied the Fourth Amendment to electronic surveillance, the Supreme Court specifically refused to extend its analysis to include domestic searches that were conducted for national security purposes. *Katz v. United States*, 389 U.S. 347, 358 n. 23 (1967); see also *Mitchell v. Forsyth*, 472 U.S. 511, 531 (1985). Later, however, in *United States v. United States District Court for the Eastern District of Michigan*, 407 U.S. 297, 299 (1972) ("*Keith*"), the Court held that the warrant requirement should apply to cases of terrorism by purely domestic groups. In doing so, the Justices framed the question by explaining that, "[i]ts resolution is a matter of national concern, requiring sensitivity both to the Government's right to protect itself from unlawful subversion and attack and to the citizen's right to be secure in his privacy against unreasonable Government intrusion." *Id.* While acknowledging that "unless Government safeguards its own capacity to function and to preserve the security of its people, society itself could become so disordered that all rights and liberties would be endangered," *id.* at

312, the Court cautioned that "[t]he danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.' Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent." *Id.* at 314. As a result, the Court held that the absence of neutral and disinterested magistrates governing the reasonableness of the search impermissibly left "those charged with [the] investigation and prosecutorial duty [as] the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks." *Id.* at 317.

The Court explicitly noted, however, that it was not considering the scope of the President's surveillance power with respect to the activities of foreign powers within or without the country. *Id.* at 308. After *Keith*, lower courts have recognized that when the government conducts a search for national security reasons of a foreign power or its agents, it need not meet the same requirements that would normally apply in the context of a search of United States citizens who are not foreign agents or for criminal law enforcement purposes. In *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980), for example, the Fourth Circuit observed that "the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would, following *Keith*, 'unduly frustrate,' the President in carrying out his foreign affairs responsibilities." *Id.* at 913. The Court based this determination on a number of factors, including:

(1) "[a] warrant requirement would reduce the flexibility of executive foreign intelligence initiatives, in some cases delay executive response to foreign intelligence threats, and increase the chance of leaks regarding sensitive executive operations," *id.*;

(2) "the executive possesses unparalleled expertise to make the decision whether to conduct foreign intelligence surveillance, whereas the judiciary is largely inexperienced in making the delicate and complex decisions that lie behind foreign intelligence surveillance Few, if any, district courts would be truly competent to judge the importance of particular information to the security of the United States or the 'probable cause' to demonstrate that the government in fact needs to recover that information from one particular source," *id.* at 913-14; and

(3) the executive branch "is also constitutionally designated as the pre-eminent authority in foreign affairs." *Id.* at 914.

The Court also recognized, however, that "because individual privacy interests are severely compromised any time the government conducts surveillance without prior judicial approval, this foreign intelligence exception to the Fourth Amendment warrant requirement must be carefully limited to those situations in which the interests of the executive are paramount." *Id.* at 915. See also *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973), cert. denied, 415 U.S. 960 (1974); *United States v. Buck*, 548 F.2d 871 (9th Cir.), cert. denied, 434 U.S. 890 (1977); *United States v. Clay*, 430 F.2d 165 (5th Cir. 1970), rev'd on other grounds, 403 U.S. 698 (1971).

Therefore, the Fourth Circuit held that the government was relieved of the warrant requirement when (1) the object of the search or surveillance is a foreign power, its agent or collaborators since such cases are "most likely to call into play difficult and subtle judgments about foreign and military affairs," 629 F.2d at 915; and (2) "when the surveillance is conducted 'primarily' for foreign intelligence reasons . . . because once surveillance becomes primarily a criminal investigation, the courts are entirely competent to make the usual probable cause determination, and because, importantly, individual privacy interests come to the fore and government foreign policy concerns recede when the government is primarily attempting to form the basis for a criminal prosecution." *Id.*

As the attacks on September 11, 2001 revealed, the government interest in conducting searches related to fighting terrorism is perhaps of the highest order -- the need to defend the nation from direct attack. As the Supreme Court has said, "It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the nation." *Haig v. Agee*, 453 U.S. 280, 307 (1981). The compelling nature of the government's interest here may be understood in light of the Founders' express intention to create a federal government "cloathed with all the powers requisite to the complete execution of its trust." *The Federalist* No. 23, at 147 (Alexander Hamilton) (Jacob E. Cooke ed. 1961). Foremost among the objectives committed to that trust by the Constitution is the security of the nation. As Hamilton explained in arguing for the Constitution's adoption, because "the circumstances which may affect the public safety" are not "reducible within certain determinate limits,"

it must be admitted, as a necessary consequence, that there can be no limitation of that authority, which is to provide for the defence and protection of the community, in any matter essential to its efficacy.

Id. at 147-48.¹ Within the limits that the Constitution itself imposes, the scope and distribution of the powers to protect national security must be construed to authorize the most efficacious defense of the nation and its interests in accordance "with the realistic purposes of the entire instrument." *Lichter v. United States*, 334 U.S. 742, 782 (1948). Nor is the authority to protect national security limited to that necessary "to victories in the field." *Application of Yamashita*, 327 U.S. 1, 12 (1946). The authority over national security "carries with it the inherent power to guard against the immediate renewal of the conflict." *Id.*

¹See also *The Federalist* No. 34, at 211 (Alexander Hamilton) (Jacob E. Cooke ed., 1961) (Federal government is to possess "an indefinite power of providing for emergencies as they might arise"); *The Federalist* No. 41, at 269 (James Madison) ("Security against foreign danger is one of the primitive objects of civil society. . . . The powers requisite for attaining it, must be effectually confided to the federal councils.") Many Supreme Court opinions echo Hamilton's argument that the Constitution presupposes the indefinite and unpredictable nature of "the circumstances which may affect the public safety," and that the federal government's powers are correspondingly broad. See, e.g., *Dames & Moore v. Regan*, 453 U.S. 654, 662 (1981) (noting that the President "exercis[es] the executive authority in a world that presents each day some new challenge with which he must deal"); *Hamilton v. Regents*, 293 U.S. 245, 264 (1934) (Federal government's war powers are "well-nigh limitless" in extent); *Stewart v. Kahn*, 78 U.S. (11Wall.) 493, 506 (1870) ("The measures to be taken in carrying on war . . . are not defined [in the Constitution]. The decision of all such questions rests wholly in the discretion of those to whom the substantial powers involved are confided by the Constitution."); *Miller v. United States*, 78 U.S. (11Wall.) 268, 305 (1870) ("The Constitution confers upon Congress expressly power to declare war, grant letters of marque and reprisal, and make rules respecting captures on land and water. Upon the exercise of these powers no restrictions are imposed. Of course the power to declare war involves the power to prosecute it by all means and in any manner in which war may be legitimately prosecuted.").

The text, structure and history of the Constitution establish that the Founders entrusted the President with the primary responsibility, and therefore the power, to ensure the security of the United States in situations of grave and unforeseen emergencies. Intelligence gathering is a necessary function that enables the President to carry out that authority. The Constitution, for example, vests in the President the power to deploy military force in the defense of United States by the Vesting Clause, U.S. Const. Art. II, § 1, cl. 1, and by the Commander in Chief Clause, *id.*, § 2, cl. 1.² Intelligence operations, such as electronic surveillance, often are necessary and proper for the effective deployment and execution of military force against terrorists. Further, the Constitution makes explicit the President's obligation to safeguard the nation's security by whatever lawful means are available by imposing on him the duty to "take Care that the Laws be faithfully executed." *Id.*, § 3. The implications of constitutional text and structure are confirmed by the practical consideration that national security decisions often require the unity in purpose and energy in action that characterize the Presidency rather than Congress.³

²See *Johnson v. Eisentrager*, 339 U.S. 763, 789 (1950) (President has authority to deploy United States armed forces "abroad or to any particular region"); *Fleming v. Page*, 50 U.S. (9 How.) 603, 615 (1850) ("As commander-in-chief, [the President] is authorized to direct the movements of the naval and military forces placed by law at his command, and to employ them in the manner he may deem most effectual"); *Loving v. United States*, 517 U.S. 748, 776 (1996) (Scalia, J., concurring in part and concurring in judgment) (The "inherent power" of the Commander in Chief "are clearly extensive."); *Maul v. United States*, 274 U.S. 501, 515-16 (1927) (Brandeis & Holmes, JJ., concurring) (President "may direct any revenue cutter to cruise in any waters in order to perform any duty of the service"); *Commonwealth of Massachusetts v. Laird*, 451 F.2d 26, 32 (1st Cir. 1971) (the President has "power as Commander-in-Chief to station forces abroad"); *Ex parte Vallandigham*, 28 F.Cas. 874, 922 (C.C.S.D. Ohio 1863) (No. 16,816) (in acting "under this power where there is no express legislative declaration, the president is guided solely by his own judgment and discretion"); *Authority to Use United States Military Forces in Somalia*, 16 Op. O.L.C. 6, 6 (1992) (Barr, A.G.).

³As Alexander Hamilton explained in *The Federalist* No. 74, "[o]f all the cares or concerns of government, the direction of war most peculiarly demands those qualities which distinguish the exercise of power by a single hand." *The Federalist* No. 74, at 500 (Alexander Hamilton) (Jacob E. Cooke ed., 1961). And James Iredell (later an

Judicial decisions since the beginning of the Republic confirm the President's constitutional power and duty to repel military action against the United States and to take measures to prevent the recurrence of an attack. As Justice Joseph Story said long ago, "[i]t may be fit and proper for the government, in the exercise of the high discretion confided to the executive, for great public purposes, to act on a sudden emergency, or to prevent an irreparable mischief, by summary measures, which are now found in the text of the laws." *The Apollon*, 22 U.S. (9 Wheat.) 362, 366-67 (1824). The Constitution entrusts the "power [to] the executive branch of the Government to preserve order and insure the public safety in times of emergency, when other branches of the Government are unable to function, or their functioning would itself threaten the public safety." *Duncan v. Kahanamoku*, 327 U.S. 304, 335 (1946) (Stone, C.J., concurring). If the President is confronted with an unforeseen attack on the territory and people of the United States, or other immediate, dangerous threat to American interests and security, it is his constitutional responsibility to respond to that threat. See, e.g., *The Prize Cases*, 67 U.S. (2 Black) 635, 668 (1862) ("If a war be made by invasion of a foreign nation, the President is not only authorized but bound to resist force by force . . . without waiting for any special legislative authority."); *Kahanamoku*, 327 U.S. at 336 (Stone, C.J., concurring) ("Executive has broad discretion in determining when the public emergency is such as to give rise to the necessity" for emergency measures); *United States v. Smith*, 27 F. Cas. 1192, 1230 (C.C.D.N.Y. 1806) (No. 16,342) (Paterson, Circuit Justice) (regardless of statutory authorization, it is "the duty . . . of the executive magistrate . . . to repel an invading foe"); see also 3 Story, *Commentaries* § 1485 ("[t]he command and application of

Associate Justice of the Supreme Court) argued in the North Carolina Ratifying Convention that "[f]rom the nature of the thing, the command of armies ought to be delegated to one person only. The secrecy, despatch, and decision, which are necessary in military operations, can only be expected from one person." Debate in the North Carolina Ratifying Convention, in 4 Jonathan Elliott, *The Debates in the Several State Conventions on the Adoption of the Federal Constitution* 107 (2d ed. Ayer Company, Publishers, Inc. 1987) (1888). See also 3 Joseph Story, *Commentaries on the Constitution* § 1485, at 341 (1833) (in military matters, "[u]nity of plan, promptitude, activity, and decision, are indispensable to success; and these can scarcely exist, except when single magistrate is entrusted exclusively with the power").

the public force . . . to maintain peace, and to resist foreign invasion" are executive powers).

The Department believes that the President's constitutional responsibility to defend the Nation may justify reasonable, but warrantless, counter-intelligence searches. As the Commander-in-Chief, the President must be able to use whatever means necessary to prevent attacks upon the United States; this power, by implication, includes the authority to collect information necessary for its effective exercise.

This examination demonstrates that the current situation, in which Congress has recognized the President's authority to use force in response to a direct attack on the American homeland, has demonstrated the government's increased interest. The government's interest has changed from merely conducting foreign intelligence surveillance to counter intelligence operations by other nations, to one of preventing terrorist attacks against American citizens and property within the continental United States itself. The courts have observed that even the use of deadly force is reasonable under the Fourth Amendment if used in self-defense or to protect others. See, e.g., *Romero v. Board of County Commissioners*, 60 F.3d 702 (10th Cir. 1995), cert. denied 516 U.S. 1073 (1996); *O'Neal v. DeKalb County*, 850 F.2d 653 (11th Cir. 1988). Here, for Fourth Amendment purposes, the right to self-defense is not that of an individual, but that of the nation and of its citizens. Cf. *In re Neagle*, 135 U.S. 1 (1890); *The Prize Cases*, 67 U.S. (2 Black) 635 (1862). If the government's heightened interest in self-defense justifies the use of deadly force, then it certainly would also justify warrantless searches.

III

It is against this background that the change to FISA should be understood. Both the executive branch and the courts have recognized that national security searches against foreign powers and their agents need not comport with the same Fourth Amendment requirements that apply to domestic criminal investigations. FISA embodies the idea that, in this context, the Fourth Amendment applies differently than in the criminal context. Nonetheless, FISA itself is not required by the Constitution, nor is it necessarily the case that its current standards match exactly to Fourth Amendment standards. Rather, like the warrant process in the normal criminal context, FISA represents a statutory procedure that, if used, will create a presumption that the surveillance is reasonable under the Fourth

Amendment. Thus, it is wholly appropriate to amend FISA to ensure that its provisions parallel the bounds of the Fourth Amendment's reasonableness test.

The national security and foreign intelligence elements of the search justify its exemption from the standard law enforcement warrant process. After the enactment of FISA, for example, courts have emphasized the distinction between searches conducted to collect foreign intelligence and those undertaken for pursuing criminal prosecutions. Although this may be due, in part, to a statutory construction of the FISA provisions, these courts' language may be seen as having broader application. As the Second Circuit has emphasized, although courts, even prior to the enactment of FISA, concluded that the collection of foreign intelligence information constituted an exception to the warrant requirement, "the governmental interests presented in national security investigations differ substantially from those presented in traditional criminal prosecutions." *United States v. Duggan*, 743 F.2d 59, 72 (2d Cir. 1984). The *Duggan* Court held that FISA did not violate the Fourth Amendment because the requirements of FISA "provide an appropriate balance between the individual's interest in privacy and the government's need to obtain foreign intelligence information." *Id.* at 74. The Court's holding was made in the context of acknowledging the reasonableness of "the adoption of prerequisites to surveillance that are less stringent than those precedent to the issuance of a warrant for a criminal investigation." *Id.* at 73.

Similarly, the Ninth Circuit found that the lowered probable cause showing required by FISA is reasonable because, although the application need not state that the surveillance is likely to uncover evidence of a crime, "the purpose of the surveillance is not to ferret out criminal activity but rather to gather intelligence, [and therefore] such a requirement would be illogical." *United States v. Cavanagh*, 807 F.2d 787, 790-91 (9th Cir. 1987) (Kennedy, J.).⁴ And consistent with both the language of the Second and Ninth Circuits, the First Circuit, in upholding the constitutionality of FISA, explained that "[a]lthough evidence obtained under FISA subsequently may be used in criminal prosecutions, the investigation of criminal activity cannot be the primary purpose of the surveillance [and therefore] [t]he act is not to be used as an end-run around the

⁴The Ninth Circuit has reserved the question of whether the "primary purpose" test is too strict. *United States v. Sarkissian*, 841 F.2d 959, 964 (9th Cir. 1988).

Fourth Amendment's prohibition of warrantless searches." *United States v. Johnson*, 952 F.2d 656, 572 (1st Cir. 1992) (citations omitted), cert. denied, 506 U.S. 816 (1992).

On the other hand, it is also clear that while FISA states that "the" purpose of a search is for foreign surveillance, that need not be the only purpose. Rather, law enforcement considerations can be taken into account, so long as the surveillance also has a legitimate foreign intelligence purpose. FISA itself makes provision for the use in criminal trials of evidence obtained as a result of FISA searches, such as rules for the handling of evidence obtained through FISA searches, 50 U.S.C. § 1801(h) & 1806, and procedures for deciding suppression motions, *id.* § 1806(e). In approving FISA, the Senate Select Committee on Intelligence observed: "U.S. persons may be authorized targets, and the surveillance is part of an investigative process often designed to protect against the commission of serious crimes such as espionage, sabotage, assassinations, kidnapping, and terrorist acts committed by or on behalf of foreign powers. Intelligence and criminal law enforcement tend to merge in this area." S. Rep. No. 95-701, at 10-11 (1978). The Committee also recognized that "foreign counterintelligence surveillance frequently seeks information needed to detect or anticipate the commission of crimes," and that "surveillance conducting under [FISA] need not stop once conclusive evidence of a crime is obtained, but instead may be extended longer where protective measures other than arrest and prosecution are more appropriate." *Id.* at 11.

The courts agree that the gathering of counter-intelligence need not be the only purpose of a constitutional FISA search. An "otherwise valid FISA surveillance is not tainted simply because the government can anticipate that the fruits of such surveillance may later be used, as allowed by § 1806(b), as evidence in a criminal trial." *Duggan*, 743 F.2d at 78. This is due to the recognition that "in many cases the concerns of the government with respect to foreign intelligence will overlap those with respect to law enforcement." *Id.* In order to police the line between legitimate foreign intelligence searches and pure domestic law enforcement operations, most courts have adopted the test that the "primary purpose" of a FISA search is to gather foreign intelligence. See *id.*; *United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991); *United States v. Pelton*, 835 F.2d 1067 (4th Cir. 1987), cert. denied, 486 U.S. 1010 (1988); *United States v. Badia*, 827 F.2d 1458, 1464 (11th Cir. 1987), cert. denied, 485 U.S. 937 (1988). Not all courts, however, have felt compelled to adopt the primary purpose test. The Ninth Circuit

has explicitly reserved the question whether the "primary purpose" is too strict and the appropriate test is simply whether there was a legitimate foreign intelligence purpose. *United States v. Sarkissian*, 841 F.2d 959, 964 (9th Cir. 1988). No other Circuit has held that such a formulation would be unconstitutional.

In light of this case law and FISA's statutory structure, we do not believe that an amendment of FISA from "the" purpose to "a significant" purpose would be unconstitutional. So long as the government has a legitimate objective in obtaining foreign intelligence information, it should not matter whether it also has a collateral interest in obtaining information for a criminal prosecution. As courts have observed, the criminal law interests of the government do not taint a FISA search when its foreign intelligence objective is primary. This implies that a FISA search should not be invalid when the interest in criminal prosecution is significant, but there is still a legitimate foreign intelligence purpose for the search. This concept flows from the courts' recognition that the concerns of government with respect to foreign policy will often overlap with those of law enforcement.

Further, there are other reasons that justify the constitutionality of the proposed change to FISA. First, as an initial matter, the alteration in the statute could not be facially unconstitutional. As the Court has held, in order to succeed a facial challenge to a statute must show that the law is invalid "in every circumstance." *Babbitt v. Sweet Home Chapter*, 515 U.S. 687, 699 (1995). As the Court made clear in *United States v. Salerno*, 481 U.S. 739 (1987), "[a] facial challenge to a legislative Act is, of course, the most difficult challenge to mount successfully, since the challenger must establish that no set of circumstances exists under which the Act would be valid." *Id.* at 745. Such a challenge would fail here. Even if FISA were amended to require that "a" purpose for the search be the collection of foreign intelligence, that class of searches would continue to include both searches in which foreign intelligence is the only purpose and searches in which it is the primary purpose -- both permissible under current case law. A fortiori, if amending FISA to "a" purpose would be constitutional, then changing the language to "a significant" purpose -- a somewhat higher standard -- would meet Fourth Amendment requirements as well.

Second, amending FISA would merely have the effect of changing the statute to more closely track the Constitution. Courts have recognized that the executive branch has the authority to conduct warrantless searches for foreign intelligence purposes, so long as

they are reasonable under the Fourth Amendment. Although the few courts that have addressed the issue have followed a primary purpose test, it is not clear that the Constitution, FISA, or Supreme Court case law requires that test. We believe that the primary purpose test is more demanding than that called for by the Fourth Amendment's reasonableness requirement. Adopting the proposed FISA amendment will continue to make clear that the government must have a legitimate foreign surveillance purpose in order to conduct a FISA search. It would also recognize that because the executive can more fully assess the requirements of national security than can the courts, and because the President has a constitutional duty to protect the national security, the courts should not deny him the authority to conduct intelligence searches even when the national security purpose is secondary to criminal prosecution.

The FISA amendment would not permit unconstitutional searches. A FISA court still remains an Article III court. As such, it still has an obligation to reject FISA applications that do not truly qualify for the relaxed constitutional standards applicable to national security searches. Rejecting an individual application, however, would not amount to a declaration that the "a significant" purpose standard was unconstitutional. Rather, the Court would only be interpreting the new standard so as not to violate the Constitution, in accordance with the canon of statutory construction that courts should read statutes to avoid constitutional difficulties. See *Public Citizen v. Department of Justice*, 491 U.S. 440, 466 (1989); *Edward J. DeBartolo Corp. v. Florida Gulf Coast Building & Construction Trades Council*, 485 U.S. 568, 575 (1988). Amending FISA to require only "a" purpose merely removes any difference between the statutory standard for reviewing FISA applications and the constitutional standard for national security searches.

Third, it is not unconstitutional to establish a standard for FISA applications that may be less demanding than the current standard, because it seems clear that the balance of Fourth Amendment considerations has shifted in the wake of the September 11 attacks. As discussed earlier in this memo, the reasonableness of a search under the Fourth Amendment depends on the balance between the government's interests and the privacy rights of the individuals involved. As a result of the direct terrorist attacks upon the continental United States, the government's interest has reached perhaps its most compelling level, that of defending the Nation from assault. This shift upward in governmental interest has the effect of expanding the class of reasonable searches under the Fourth

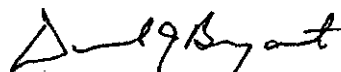
Amendment. Correspondingly, changing the FISA standard to "a significant" purpose will allow FISA warrants to issue in that class of searches. A lower standard also recognizes that, as national security concerns in the wake of the September 11 attacks have dramatically increased, the constitutional powers of the executive branch have expanded, while judicial competence has correspondingly receded. Amending FISA only recognizes that the Fourth Amendment analysis has changed in light of the more compelling nature of the government's interests given the altered national security environment.

Fourth, amending FISA in this manner would be consistent with the Fourth Amendment because it only adapts the statutory structure to a new type of counter-intelligence. FISA was enacted at a time when there was a clear distinction between foreign intelligence threats, which would be governed by more flexible standards, and domestic law enforcement, which was subject to the Fourth Amendment's requirement of probable cause. Even at the time of the act's passage in 1978, however, there was a growing realization that "intelligence and criminal law enforcement tend to merge in [the] area" of foreign counterintelligence and counterterrorism. S. Rep. No. 95-701, at 11. September 11's events demonstrate that the fine distinction between foreign intelligence gathering and domestic law enforcement has broken down. Terrorists, supported by foreign powers or interests, had lived in the United States for substantial periods of time, received training within the country, and killed thousands of civilians by hijacking civilian airliners. The attack, while supported from abroad, was carried out from within the United States itself and violated numerous domestic criminal laws. Thus, the nature of the national security threat, while still involving foreign control and requiring foreign counterintelligence, also has a significant domestic component, which may involve domestic law enforcement. Fourth Amendment doctrine, based as it is ultimately upon reasonableness, will have to take into account that national security threats in future cannot be so easily cordoned off from domestic criminal investigation. As a result, it is likely that courts will allow for more mixture between foreign intelligence gathering and domestic criminal investigation, at least in the counter-terrorism context. Changing the FISA standard from "the" purpose to "a significant" purpose would be consistent with this likely development.

For the foregoing reasons, we believe that changing FISA's requirement that "the" purpose of a FISA search be to collect foreign intelligence to "a significant" purpose will not violate the Constitution. We hope that making the Committee aware of the

Department's views is helpful to its deliberation. Please do not hesitate to contact my office if we may be of further 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 dark ink, appearing to read "Daniel J. Bryant". The signature is fluid and cursive, with the first name "Daniel" and last name "Bryant" clearly distinguishable.

Daniel J. Bryant
Assistant Attorney General

AN IDENTICAL LETTER HAS BEEN SENT TO THE HONORABLE RICHARD SHELBY, VICE CHAIRMAN, SELECT COMMITTEE ON INTELLIGENCE; THE HONORABLE PATRICK J. LEAHY, CHAIRMAN, COMMITTEE ON THE JUDICIARY; AND THE HONORABLE ORRIN G. HATCH, RANKING MINORITY MEMBER, COMMITTEE ON THE JUDICIARY



U.S. Department of Justice

Office of Legislative Affairs

Washington, D.C. 20530

September 27, 2001

The Honorable John A. Boehner
Chairman
Committee on Education and
the Workforce
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

The Department of Justice has reviewed both the House-passed and Senate-passed versions of H.R. 1, per your request. We support the inclusion of the provision authored by Senator Biden relating to the COPS in Schools program and offer technical suggestions concerning the description of duties and activities of the School Resource Officer under that provision. We also have identified two categories of constitutional issues, and have additional policy concerns which are addressed below. An identical letter is being sent to Senator Edward Kennedy, Chairman, Senate Committee on Health, Education, Labor, and Pensions.

1. Biden provision reauthorizing Cops in Schools program

The Department of Justice strongly supports the inclusion of section 1027 of the Senate bill, as authored by Senator Biden, to authorize the "COPS in Schools" program for five additional years, and which also provides resources to make our nation's schools safer. This provision provides the authority to grant local law enforcement agencies federal resources to hire additional school resource officers (SRO's). Since its inception in 1998, this program has provided grants to fund the addition of 3,600 SRO's in more than 1,700 communities across the country. This section will help ensure that this valuable program continues to provide communities with the opportunity to make their schools safer.

The Department of Justice supports the role of the SRO and its link with community policing. However, section 1027 of the Senate bill represents a change in the statutory definition of a SRO and this link. See 42 U.S.C. 3796dd-8. Currently, the primary role of an SRO is to ensure the safety and security of students and staff, and the SRO accomplishes this by striking a fine balance between his enforcement, intervention, and prevention activities. The new duties as described in section 1027 appear to shift the SRO away from being a community policing officer and also provides that it is the role of an SRO to trace guns through the Bureau of Alcohol, Tobacco, and Firearms. In order to avoid any possible federalism issues that may be created by requiring the local SRO to work

with the federal BATF, we suggest striking paragraphs "I" and "J" This will give local law enforcement added flexibility to create community policing plans that work best in its schools without specific requirements from the federal government on how to deploy that officer.

Finally, we suggest inserting "educators" into proposed subparagraph (E) of §1709 (4)(1) of Title I of the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3796dd-8(4) and "teachers and staff" into proposed subparagraph (H). These changes more accurately reflect the composition of most safe schools partnerships.

2. Requirements in both bills that Executive Branch officials provide Congress with draft legislation or legislative policy recommendations

The Recommendations Clause of the Constitution grants to the President the authority to make those legislative recommendations that he, in his discretion, deems appropriate and necessary. *See* U.S. Const. art. II, § 3 (the President "shall from time to time . . . recommend to [Congress's] Consideration such Measures as he shall judge necessary and expedient"). Requirements that the President or his subordinates submit draft legislation or legislative policy recommendations typically infringe on prerogatives reserved to the President by the Recommendations Clause.

We have identified four provisions of the engrossed bills that raise Recommendations Clause concerns. Section 313 of the House bill, which proposes amendments to Title XI of the Education Amendments of 1978, 25 U.S.C. §§ 2001 *et seq.* (2000), would call on the Secretary of the Interior to provide Congress with recommendations concerning future uses of certain educational funds and future financing of tribally controlled community colleges, and with biannual "suggestions for the improvement of the Bureau [of Indian Affairs] educational system and for increasing tribal or local Indian control of such system." H.R. 1 (House) § 313 (proposed Education Amendments of 1978 § 1136(a)). Section 201 of the Senate bill, which proposes amendments to Title II of the Elementary and Secondary Education Act of 1965 (ESEA), would call for a report to Congress from the Secretary of Education containing recommendations regarding expansion of a pilot project to recruit and retain master teachers. *See* H.R. 1 (Senate) § 201 (proposed ESEA § 2123(b)(7)(B)(ii)(II)). Section 409 of the Senate bill would amend the ESEA to provide for a study by the Secretary of Education and the Director of the Centers for Disease Control and Prevention that would include recommendations to Congress concerning federal assistance to schools that violate federal and state health and safety standards. *See id.* § 409 (proposed ESEA § 4801(b)(3)). Finally, section 1016(b) of the Senate bill would call for a report to Congress from the Secretary of Education and the Attorney General containing "recommendations and legislative remedies for the problem of sexual abuse in schools." *See id.* § 1016(b).

To the extent that these provisions obligate Executive Branch officials to provide Congress with draft legislation or legislative policy recommendations, they threaten to infringe on prerogatives reserved to the President by the Recommendations Clause. To avoid the constitutional difficulties that such interpretations would create, we recommend that the provisions be revised to say that the relevant Executive Branch officials provide the legislative proposals “as may be appropriate.”

3. *The House bill’s requirement that the Secretary of Education award grants “pursuant to the recommendations” of the Pacific Region Educational Laboratory*

Section 108 of the House bill would provide for federal educational grants to the outlying areas and freely associated States. Proposed ESEA section 1121(b)(3)(B) states that the Secretary “shall award grants . . . on a competitive basis, *pursuant to* the recommendations of the Pacific Region Educational Laboratory [the PREL] in Honolulu, Hawaii” (emphasis added). Under this provision, the Secretary, although legally responsible for making the grants (and likely to be held politically accountable for the choice of recipients), would apparently be obliged to implement decisions made by an independent educational laboratory. See § 941(h) of the Educational Research, Development, Dissemination, and Improvement Act of 1994, Title IX of Pub.L. No. 103-227, 108 Stat. 250 (codified as amended at 20 U.S.C. § 6041(h) (2000)) (providing for Department of Education to contract for services of regional educational laboratories). Although the provision’s language characterizes the views of the PREL as “recommendations,” which would suggest that they are merely advisory, the statement that the Secretary “shall” make awards “pursuant to” the PREL’s actions might be read to make those views legally binding.

To avoid any constitutional problems that might result from such a separation of control and accountability and from delegation of substantive decision-making authority to the PREL, we recommend modification of this provision to ensure that the Secretary retains appropriate control over awards of grants. The parallel provision of the Senate bill, section 120D, accomplishes this in proposed ESEA § 1121 (b)(2)(A) by instructing the Secretary to “tak[e] into consideration the recommendations of the Pacific Region Educational Laboratory” in awarding grants.

4. *Concerns on the Senate bill’s provisions regarding “School Safety and Violence Prevention”*

Proposed ESEA section 4305(a), under section 403(a) of the Senate-passed version of H.R. 1, would establish a School Security Technology and Resource Center (the Center) at the Sandia National Laboratories by creating a partnership between three existing centers: the Sandia National Laboratories (Sandia) in Albuquerque, New Mexico; the National Law Enforcement and Corrections Technology Center-Southeast (NLECTC-SE) in Charleston, South Carolina; and the National Center

for Rural Law Enforcement (NCRLE) in Little Rock, Arkansas. DOJ opposes this proposal because it would impose a new layer of bureaucracy on an activity that is already government-funded and monitored, and it would double the federal funding authorized for school security technology activities at these 3 centers from approximately \$5 million per year to nearly \$10 million per year.

Since FY 1999, NCRLE has been a Bureau of Justice Assistance (BJA) grantee, and Sandia and NLECTC-SE have been National Institute of Justice (NIJ) grantees. In fact, NIJ presently funds 6 NLECTCs – 1 national and 5 regional centers. Each regional center examines the school security technology needs of its own geographical area and provides technical expertise in one or more specific areas of security technology. The NLECTC national center in Rockville, Maryland operates a variety of information and referral services including JUSTNET, the Justice Technology Information Network and Internet Web site, which links users to the entire NLECTC system. Thus, the NLECTC system serves as a national repository of information on all public safety technology needs, including school safety. The Senate version of H.R. 1 would peel off the NLECT Center in Charleston, South Carolina and incorporate it into a new partnership with only Sandia, and NCRLE. We are concerned that doing so will undermine the informal partnership that already exists among Sandia, NLECTC-SE and the other centers in the NLECTC system; and NCRLE. Through this existing partnership, officials from the Department of Justice, the Department of Education, and the Department of Energy coordinate their school security technology efforts. To our knowledge, neither federal officials nor local school district officials have articulated the need for a formal agreement among the federal agencies to create a “School Security Technology and Resource Center.” We believe that creating such a center would not result in better coordination among the grantees, but would only formalize the structure that is already working to the satisfaction of federal and local officials.

Our second reason for opposing the Senate proposal to create a school security technology center is the cost. Proposed section 4305(d) would authorize \$4.75 million in appropriations for each of fiscal years 2002, 2003, and 2004. Specifically, for each year, \$2 million would be authorized for Sandia, \$2 million for NCRLE, and \$750,000 for NLECTC-SE. The proposal to create and fund a new “school technology partnership” should be evaluated in light of the federal funds already dedicated to school security technology through DOJ grants:

Sandia, New Mexico - monies administered by NIJ

FY 1999 - \$273,840 earmark in COPS appropriations

FY 2000 - \$1 million earmark in COPS appropriations

FY 2001 - \$498,900 earmark in COPS appropriations

Subtotal - \$1.75 million

FY 2002 - \$2 million earmark for “New Mexico School Security Technology and Resource Center” (presumably Sandia) included in Senate Appropriations Report

NLECTC - NIJ discretionary monies administered by NIJ

FY 1999 - \$2,177,072 (\$558,072 to NLECTC-SE in Charleston, South Carolina)

FY 2000 - \$1 million (\$260,775 to NLECTC-SE)

FY 2001 - \$1.8 million (\$552,781 to NLECTC-SE)

Subtotal - \$5 million

FY 2002 - NIJ will decide the amount of NLECTC funding based on the level of discretionary funds available in its FY 2002 appropriation.

NCRLE, Little Rock, Arkansas - monies administered by BJA

FY 2000 - \$2 million

FY 2001 - \$1,995,600

Subtotal - \$4 million

FY 2002 - \$3 million earmark in COPS appropriations for "School Violence Resource Center" (presumably NCRLE) included in Senate Appropriations Report.

To date, Congress has appropriated a total of nearly \$10.75 million dollars for school security technology activities through DOJ NLECTC and NCRLE grants. This total includes approximately \$1.75 million for the School Security Technology and Resource Center at Sandia in New Mexico, \$5 million for the National Law Enforcement and Corrections Technology Centers (NLECTCs), and \$4 million for NCRLE. In FY 2002, Congress appears ready to appropriate another \$5 million through DOJ for activities specific to Sandia and the NCRLE. If the Senate's proposed ESEA section 4305 also is funded, then, in FY 2002, funding for Sandia (from ED and DOJ appropriations) will jump from \$2 million to \$4 million, and funding for NCRLE (again, from ED and DOJ appropriations) also will increase from \$2 million to \$4 million.

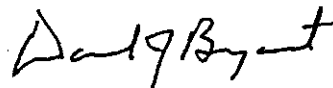
DOJ is concerned that section 4305(c) would undermine the role of Sandia and NLECTC in *evaluating* and *recommending* security technologies by allowing Sandia and NLECTC to *develop* school security technologies. Currently, NIJ awards grants to Sandia to *review and evaluate* security technology and provide limited technology assistance to schools. If Sandia is also permitted to *develop* particular technologies, it would be responsible for evaluating its own products and those of its competitors, an obvious and untenable conflict of interest. The legislation would create a similar conflict of interest for NLECTC-SE. Currently, NLECTC-SE is responsible for assessing the unique security needs of individual communities and then recommending security technologies strategies that can best meet those needs. If NLECTC-SE is authorized to develop its own school-security technologies, its role as an "honest broker" will be undermined. It will lose its credibility as an entity capable of objectively reviewing and evaluating security technologies. To avoid these conflicts of interest, we recommend that Sandia and NLECTC-SE not be given authority to *develop* school security technology solutions.

Additionally, in subsection 4305(c), we recommend deleting the last sentence mandating that the new Center "conduct and publish school violence research, coalesce data from victim communities, and monitor and report on schools that implement school security strategies." Our view is that assigning these tasks to the new Center would be an unwise allocation of limited federal resources because federal entities already conduct and publish school-violence research and compile victim data: DOJ's NIJ and the Office of Juvenile Justice Delinquency Prevention (OJJDP), the Department of Education (DOE) and the Centers for Disease Control and Prevention (CDC) research and publish school-violence information, and the DOE, CDC, and DOJ's Bureau of Justice Statistics (BJS) compile data from victims. Rather than authorizing additional federal monies for these purposes, perhaps the legislation should encourage greater coordination of existing school violence research, publication, and dissemination efforts.

We recommend deleting section 4306(c). It is unclear why additional funding for local school security programs is needed. Rather than creating another federal grant program, we believe it would be more efficient to add any available new funds to the law-enforcement and safe-school-grant programs already managed by the Attorney General under OJP.

Thank you for the consideration of our views. Please do not hesitate to contact us if additional assistance is needed. The Office of Management and Budget has advised that there is no objection to the submission of this letter from the standpoint of the Administration's program.

Sincerely,

A handwritten signature in black ink, appearing to read "Daniel J. Bryant". The signature is fluid and cursive, with the first name "Daniel" and last name "Bryant" clearly distinguishable.

Daniel J. Bryant
Assistant Attorney General

cc: The Honorable George Miller
Ranking Member



U. S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

August 19, 2002

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

Dear Mr. Chairman:

Thank you for your letter of August 2, 2002, and the opportunity it affords the Department to restate its commitment that it will vigorously investigate and prosecute corporate and accounting fraud matters.

To that end, within two days of enactment of the Sarbanes-Oxley Act of 2002 ("the Act"), the Department prepared and disseminated guidance giving an introductory explanation of key provisions of the Act and its new or enhanced criminal penalties. With new criminal legislation, the Department will typically prepare immediate guidance for prosecutors to alert them to the new provisions and to begin the process of incorporating those new laws into our investigations and prosecutions. In no respect, however, was this guidance on the Act intended to narrow enforcement of any of its provisions. Indeed, the Department's cover memo of August 1, 2002, unambiguously states: "As the President has emphasized, it is vital that all components of the Department of Justice, including our United States Attorneys' Offices and Federal Bureau of Investigation Field Offices, work together to ensure that we take full advantage of the provisions of this new law to enhance our prosecution of significant financial crimes."

The guidance is only the first step in what will be a comprehensive effort to prepare and train our agents and prosecutors to meet the challenges posed by complex corporate criminal activity. In the months to come, the Department will prepare training materials, conduct training sessions, and examine whether amendments to the United States Attorneys Manual are necessary to address these new criminal provisions and enhanced criminal penalties, and the Department will keep you advised of our progress in this process. The Department will also work closely with the United States Sentencing Commission as it expeditiously reviews and, it is anticipated, revises the sentencing guidelines as directed by several provisions of the Act.

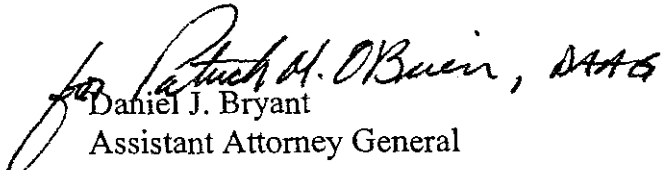
With respect to your concerns regarding specific discussion of new Section 1519 of Title 18, United States Code, and the insertion of a new subsection (c) in Section 1512, rest assured that the guidance was not intended to link the substantive elements of the former provision with the elements of the latter. Rather, the guidance appropriately directs prosecutors to consider both provisions and determine which is more appropriate in each particular factual situation. Contrary to the implication in your letter, the guidance at page 1 unequivocally states that new section 1519 applies to "any 'matters' within the jurisdiction of any department or agency of the United States, or any bankruptcy proceeding, or in relation to or contemplation of any such matter or proceeding." In addition, the guidance makes clear that neither Section 1519 nor Section 1512(c) requires a "corrupt persuader."

Similarly, the guidance highlights the new securities fraud statute, Section 1348 of Title 18, United States Code, which provides a direct statutory prohibition complementing current antifraud provisions found in the mail and wire fraud statutes, as well as provisions of the Securities Exchange Act of 1934, codified in Title 15, United States Code.

With respect to your inquiry about the response that you and Senator Hatch sent dated July 26, 2002 regarding the Corporate Fraud Task Force, the Department is working on its response and expects to have it to you shortly.

The Department looks forward to continuing to work with you and your Committee on our continuing effort to expose and punish corporate fraud and to restore confidence in America's financial system. Please let us know if we may be of additional assistance.

Sincerely,


Daniel J. Bryant
Assistant Attorney General

cc: The Honorable Orrin G. Hatch
Ranking Minority Member



U.S. Department of Justice

Office of Legislative Affairs

Washington, D.C. 20530

December 10, 2001

The Honorable Bob Ney
Chairman
Committee on House Administration
U.S. House of Representatives
Washington, D.C. 20515

Dear Mr. Chairman:

This letter responds to your letter of November 29, 2001 regarding the effect of H.R. 3295, the "Help America Vote Act," upon the National Voter Registration Act of 1993 ("NVRA").

Although several provisions in the bill affect the list maintenance provisions in section 8 of the NVRA, it is evident that the bill is not designed to modify the NVRA and, in fact, it does not alter or undermine the NVRA's requirements. Section 903 of the bill itself specifically provides that nothing in H.R. 3295 "shall supercede, restrict or limit the application of . . . NVRA," that nothing in the bill "authorizes or requires any conduct which is prohibited by the NVRA," and that nothing in the bill "may be construed to affect the application of the . . . NVRA . . . to any State" (except as specifically provided in the bill). These provisions would guide the Department's enforcement efforts if the bill becomes law.

Various parts of the bill reference the NVRA and appear designed to clarify and strengthen enforcement of the NVRA's list maintenance provisions. Section 502(2) would require all 50 States and the District of Columbia, Puerto Rico, Guam, American Samoa, and the United States Virgin Islands to adopt a system of list maintenance ensuring that voter registration lists are accurate and updated regularly, and that removes registrants who are ineligible to vote. Under this system, "consistent with the [NVRA]," registrants who have not voted in 2 or more consecutive Federal general elections and who have not responded to a notice would be required to be removed from the list of eligible voters, except that no registrant could be removed solely by reason of failure to vote. This system also would have to have safeguards to ensure that eligible voters were not removed in error. Section 501(a)-(b) would require all States to enact

legislation to adopt such a list maintenance system, but properly would leave States discretion as to the specific methods of implementing such a system.

Section 902(a), entitled "Clarification of ability of election officials to remove registrants . . . on grounds of change of residence," would amend the NVRA's existing requirement (at 42 U.S.C. 1973gg-6(b)(2)) that any general program not result in removal of voters' names due to their "failure to vote." However, the amendment in section 902(a) merely would clarify that nothing in section 1973gg-6(b)(2) was intended to prohibit a State from using the procedures already in sections 1973gg-6(c)-(d) to remove the names of voters who have not voted or have not appeared to vote in two or more consecutive Federal general elections and who have not notified the registrar, or responded to a notice sent by the registrar, that they intend to remain registered in the jurisdiction. As an amendment to the NVRA, this provision would apply only in the 45 jurisdictions covered by the NVRA (44 States and the District of Columbia).

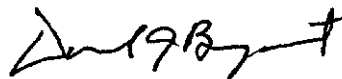
In view of the bill's several affirmations that removal of names from voter rolls should be carried out in a manner consistent with the NVRA and in view of the general affirmations in section 903 that the bill will not restrict or limit the NVRA, the bill's list maintenance provisions can and should be read consistently with the NVRA's existing list maintenance procedures, which basically are: section 1973gg-6(c) suggests the Postal Service National Change of Address program as one example of a means of identifying voters who have become ineligible because they have moved outside the jurisdiction. Section 1973gg-6(d) then provides a confirmation process that States must follow before removing voters identified as potentially ineligible due to having moved. As above, voters may be removed if: 1) they do not respond to the registrar's notice and do not vote or appear to vote in two Federal general elections; or 2) they confirm in writing that they have moved outside the jurisdiction.

Many States, following guidance from the Federal Election Commission, legislatively adopted or legislatively revised list maintenance provisions after passage of the NVRA. *See, e.g.,* Ak. Stat. 15.07.130; Fl. Stat. 98.065, 98.075, 98.093; Ga. Stat. 21-2-231 to 21-2-235; Va. Stat. 24.2-427 to 24.2-428.2. To the extent that the 45 jurisdictions covered by the NVRA have adopted list maintenance programs consistent with 42 U.S.C. 1973gg-6, we conclude that the new clarifying provisions of section 902(a) of the bill would not require those States to amend their programs. Likewise, State legislation consistent with the NVRA probably would meet the new, less specific, minimum standards for list maintenance required in section 502(2) of H.R. 3295. If this interpretation differs with that of the drafters of the bill, some clarification may be warranted.

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, appearing to read "Dan J. Bryant", with a stylized flourish at the end.

Daniel J. Bryant
Assistant Attorney General

IDENTICAL LETTER SENT TO THE HONORABLE STENY HOYER, RANKING
MINORITY MEMBER



U.S. Department of Justice

Office of Legislative Affairs

Washington, D.C. 20530

September 11, 2003

The Honorable John McCain
Chairman
Committee on Commerce, Science, and Transportation
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

This letter presents the views of the Administration on S. 877, the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" ("CAN SPAM"). The Administration supports Senate passage of S. 877, although we have some concerns which we discuss below. We regard S. 877 as an important first step in helping consumers and businesses to combat unsolicited commercial e-mail, better known as "spam," and applaud the Congress' efforts to pass legislation that helps to address this problem. The Administration agrees with the finding in section 2(a) of the bill that the problems with spam "cannot be solved by Federal legislation alone" and "the development and adoption of technological approaches and the pursuit of cooperative efforts with other countries will be necessary as well." To complement legislation, the Administration is conducting research into short- and long-term technological solutions and is convening discussions with the private sector and academia to fight spam.

The following comments, while not exhaustive, indicate the Administration's views on many of the strengths of the bill, as well as suggestions for measures intended to help consumers and businesses combat the inefficiencies and potentially harmful effects of deceptive and misleading spam. The bill would help to address some of the problems associated with the rapid growth and abuse of spam by establishing a framework of administrative, civil, and criminal enforcement tools targeted at spam, and by providing consumers with options to reduce the volume of unwanted commercial e-mail they receive. The bill would also establish important "rules of the road" for civil enforcement by the Federal Trade Commission ("FTC"), other Federal agencies, State attorneys general, and Internet service providers ("ISPs") as well as create new criminal penalties to assist in deterring the most offensive forms of spam.

Civil Protections: The Administration generally supports the bill's civil provisions that protect recipients of commercial electronic mail, including the prohibitions on using false transmission information, sending e-mail to "harvested" addresses, and retransmitting spam messages through an unlawfully accessed computer system or network. However, the Administration believes that it would be desirable for both policy and constitutional reasons for section 5 of the bill to include a materiality requirement for false or misleading header information, as is included in the

criminal provision addressing false or misleading header information found in section 4. The term "materially" should be defined to include fraudulent headers that are material to the ability of an entity having enforcement power under the bill to locate or investigate the initiator or sender of the message.

Consumer Choice: The Administration supports the pro-consumer provisions in section 5(a) of S. 877 that recognize the importance of maintaining good consumer relationships. Under the bill, consumers would have an option to choose not to receive any further unsolicited e-mail messages from a sender. Any bill must continue a careful balancing of the desire for consumers to deter commercial e-mail with the benefits that accrue from communicating to consumers the availability of potentially desirable products and services. The Administration notes, for example, that the time frame for implementation of a consumer's request to not receive further unsolicited e-mails may merit further consideration to ensure its practicability, given the disparate sizes of companies using the Internet and particular circumstances.

Statutory Caps/Class Action Suits: The Administration also supports the bill's provisions to cap statutory damages and keep such limits consistent for both ISPs and States, but believes statutory damages should be capped for all offenses, including those under section 5(a)(1) – sending e-mail with false or misleading headers. Without caps in all instances, the Administration is concerned not only that legitimate e-mail marketers may be unduly penalized with large statutory damage judgments for inadvertent violations, but also that even the prospect of uncapped damage judgments could have a chilling effect on legitimate electronic commerce. In addition, the Administration supports adding a provision to the bill that would prohibit class action suits, similar to section 104 in H.R. 2214, the "Reduction in Distribution of Spam Act of 2003."

Enforcement Authority: The Administration supports the bill's proposal to provide the FTC, other Federal functional regulators, State attorneys general, and ISPs with civil enforcement authority. The Administration believes the bill should maintain the existing regulatory authority of the Federal functional regulators regarding their respective regulated institutions.

Rulemaking Authority: The Administration supports granting the enforcement agencies in subsections 7(a) and (b) rulemaking authority to give them the necessary flexibility to respond quickly to evolving spammer techniques for which they have primary regulatory authority. The Administration also encourages the Senate to provide the FTC with the flexibility to obtain injunctive relief or issue administrative cease-and-desist orders without having to prove "knowledge" in a manner that preserves the FTC's existing authority under the FTC Act in respect of these actions.

Criminal Violations/Sanctions: The Administration supports the bill's proposal to criminalize spam that contains a header that is materially false or materially misleading. The Administration also supports adding a provision to the bill to make spam containing unmarked pornography a criminal offense. The Administration supports triggers for felony treatment similar to those

proposed in section 2(a) of S. 1293, the "Criminal Spam Act of 2003." The Administration believes these triggers would permit felony punishment for appropriately egregious offenders without imposing an effectively insurmountable burden of proof upon the Government.

The Administration supports the concept, advanced in S. 1293, that would direct the United States Sentencing Commission to consider sentencing enhancements for convicted spammers that have additionally obtained e-mail addresses by harvesting. In fact, we support a sentencing enhancement for using automated tools either to collect or to generate e-mail addresses used in the offense. The Administration also supports adding sentencing factors similar to those found in section 624(b) of H.R. 2214.

State Preemption: The Administration supports appropriate preemption of State laws that affect spam. It is important that in the criminal law arena, States are able to bring their criminal law enforcement resources to bear to combat fraudulent and unmarked pornographic spam. It is also important to provide greater certainty in interstate commerce for enterprises currently facing a wide divergence in State civil law and enforcement, while providing appropriate remedies for consumers.

Constitutional Issues: The Administration has a serious question about section 7(b)(6)'s consistency with principles of constitutional federalism and recommends that it be amended to clarify that State officials' authority to enforce the provision is permissive, not mandatory. Indeed, we presume that the drafters likely intended the current language to permit, but not to require State agencies to enforce the bill's provisions. Nevertheless, we believe that it is important to change the language to make this absolutely clear. In addition, the Administration believes that to the extent that provisions in the bill purport to require Executive branch agencies to provide Congress with legislative recommendations, they run afoul of the Constitution's Recommendations Clause. Therefore, sections 9 and 10 should be made precatory or amended to require only recommendations that the President considers "necessary and expedient."

Technical Definitions: The Administration believes the bill's definition of a "commercial electronic mail message" in section 3(2)(A) should be broadened to cover messages "a principal purpose" of which are commercial. Thus, the Administration suggests the definition read as follows: "The term 'commercial electronic mail message' means any electronic mail message a principal purpose of which is the commercial advertisement or promotion of a commercial product ..." This change would help to ensure that the majority of spam messages are covered while still excluding obviously non-commercial messages.

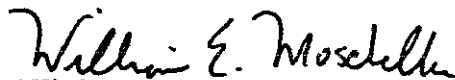
The Administration also believes the definition of "sender" in section 3(17) should be edited to state the following: "The term 'sender,' when used with respect to a commercial electronic mail message, means a person who initiates said message." It is not uncommon today for a spammer to advertise somebody else's products and services

on their own initiative in order to obtain revenues from commissions. Such a spammer would not be advertising his or her own products, services or web site, and would therefore not be covered under the bill's original definition of sender. Separately, the Administration supports expanding the definition to include a successor's interest, as is done in H.R. 2214.

The Administration notes that there may be reasons to treat recipient e-mail address information differently under the law than other header information and would be willing to provide technical advice to the Congress on this point.

The Administration applauds the Senate Commerce Committee for reporting this bill in a timely manner and looks forward to working with the Congress to enact legislation this year to help combat spam. 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,



William E. Moschella
Assistant Attorney General
Department of Justice



Theodore W. Kassinger
General Counsel
Department of Commerce

cc: The Honorable Ernest F. Hollings
Ranking Minority Member
Committee on Commerce, Science, and Transportation

The Honorable Conrad Burns
Chairman
Subcommittee on Communications
Committee on Commerce, Science, and Transportation

The Honorable Orrin G. Hatch
Chairman
Committee on the Judiciary

The Honorable Patrick J. Leahy
Ranking Minority Member
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."¹

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.

¹ 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.² 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

² 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.

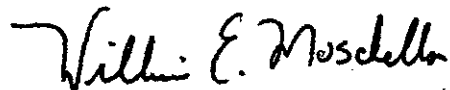
Because of this nullification, re-enactment of these amendments was necessary in § 6501 of Pub. L. 108-458, the Intelligence Reform and Terrorism Prevention Act of 2004. The purpose of the guidelines (and the related contempt sanction provision) in this legislation remains the same as in all earlier 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 fluid and cursive, with the first name "William" and last name "Moschella" clearly legible.

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.¹

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.² 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

¹ 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.

² 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.³

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

³ 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 parentheticals 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,⁴ and may do so upon the approval of the court to assist in the enforcement of state criminal law.⁵ 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) –

⁴ See Rule 6(e)(3)(A)(ii).

⁵ 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).⁶

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.⁷

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

⁶ 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).

⁷ *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

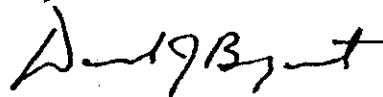
(2) inserting "and (VI)" after "Rule 6(e)(3)(C)(i)(V)".

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.