Office of the Attorney General
Washington, D. C. 20530

August 29, 2005

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

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

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

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

Dear Messrs. Chairmen:

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

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

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

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

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

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

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

Sincerely,

/s/

Alberto R. Gonzales
Attorney General

Enclosure

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

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

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

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

ENCLOSURE

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

USA PATRIOT Act Section 203(b)

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

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

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

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

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

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

USA PATRIOT Act Section 206

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

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

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

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

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

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

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

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

USA PATRIOT Act Section 207

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

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

USA PATRIOT Act Section 212

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

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

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

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

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

USA PATRIOT Act Section 213

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

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

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

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

USA PATRIOT Act Section 215

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

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

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

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

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

USA PATRIOT Act Section 505

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

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

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

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

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

Sunsets

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

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

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

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

Terrorism-Related Grant Programs

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

Additional Reporting Requirements

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

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

- The aggregate number of persons targeted for orders issued under this chapter, including a breakdown of those targeted for-electronic surveillance under section 1805 of this title; physical searches under section 1824 of this title; pen registers under section 1842 of this title; and access to records under section 1861 of this title. *See* 50 U.S.C. § 1871.

- The total number of applications made for orders and extensions of orders approving electronic surveillance under this subchapter; and the total number of such orders and extensions either granted, modified, or denied. *See* 50 U.S.C. § 1807.

- A description of each criminal case in which information acquired under this chapter has been passed for law enforcement purposes during the period covered by such report; and each criminal case in which information acquired under this chapter has been authorized for use at trial during such reporting period. *See* 50 U.S.C. § 1808.

- The total number of applications made for orders approving physical searches under this subchapter; the total number of such orders either granted, modified, or denied; and the number of physical searches which involved searches of the residences, offices, or personal property of United States persons, and the number of occasions, if any, where the Attorney General provided notice pursuant to section 1825(b) of this title. *See* 50 U.S.C. § 1826.

- The total number of applications made for orders approving the use of pen registers or trap and trace devices under this subchapter [50 U.S.C.A. § 1841 *et seq.*]; and the total number of such orders either granted, modified, or denied. *See* 50 U.S.C. § 1846.

- The total number of applications for orders approving requests for the production of tangible things under section 1861 of this title; and the total number of such orders either granted, modified, or denied. *See* 50 U.S.C. § 1862.

- A summary of significant legal interpretations of this chapter involving matters before the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review, including interpretations presented in applications or pleadings filed with the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review by the Department of Justice. *See* 50 U.S.C. § 1871.

- Copies of all decisions (not including orders) or opinions of the Foreign Intelligence Surveillance Court or Foreign Intelligence Surveillance Court of Review that include significant construction or interpretation of FISA. *See* 50 U.S.C. § 1871

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

> (d) Tariff Act of 1990—Section 596 of the Tariff Act of 1930 (19 U.S.C. § 1595a) is amended by adding at the end the following:
>
> "(d) Merchandise exported or sent from the United States or attempted to be exported or sent from the United States contrary to law, or the proceeds or value thereof, and property used to facilitate the **exporting or sending of such merchandise, the attempted exporting or sending of such merchandise, or the** receipt, purchase, transportation, concealment, or sale of such merchandise prior to exportation shall be **seized and** forfeited to the United States.".

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

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

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

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

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

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

Appendix A

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

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

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

"987. Anti-terrorist forfeiture protection."; and

(B) by inserting at the end the following:

"§ 987. Anti-terrorist forfeiture protection

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

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

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

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

~~"(c) Clarifications. –~~

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

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

~~"(B) the Constitution; or~~

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

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

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

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

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

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

U.S. Department of Justice

Office of Legislative Affairs

RECEIVED

2005 JUL -5 AM 11: 57

OIPR
DEPT OF JUSTICE

Office of the Assistant Attorney General — *Washington, D.C. 20530*

~~SECRET~~

MAY 24 2005

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

Dear Chairman Roberts:

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

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

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

Classified by: James A. Baker, Counsel for Intelligence Policy, Office of Intelligence Policy and Review, U.S. Department of Justice
Reason: 1.4(c)
Declassify on: X1

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

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

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

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

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

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

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

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

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

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

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

(b)(1)1.4c

(b)(1)1.4c

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

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

Sincerely,

William E. Moschella

William Moschella
Assistant Attorney General