Calendar No. 132

109TH CONGRESS, 1st Session | SENATE | REPORT 109–85

TO PERMANENTLY AUTHORIZE CERTAIN PROVISIONS OF THE UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM (USA PATRIOT) ACT OF 2001, TO REAUTHORIZE A PROVISION OF THE INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004, TO CLARIFY CERTAIN DEFINITIONS IN THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, TO PROVIDE ADDITIONAL INVESTIGATIVE TOOLS NECESSARY TO PROTECT THE NATIONAL SECURITY

JUNE 16, 2005.—Ordered to be printed

Mr. ROBERTS, from the Select Committee on Intelligence, submitted the following

R E P O R T

together with

ADDITIONAL AND MINORITY VIEWS

[To accompany S. 1266]

The Select Committee on Intelligence (Committee), having considered the original bill (S. 1266), to permanently authorize certain provisions of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, to reauthorize a provision of the Intelligence Reform and Terrorism Prevention Act of 2004, to clarify certain definitions in the Foreign Intelligence Surveillance Act (FISA) of 1978, to provide additional investigative tools necessary to protect the national security, and for other purposes, reports an original bill without amendment favorably thereon and recommends that the bill do pass.

PURPOSE AND SCOPE OF COMMITTEE REVIEW

The attacks of September 11, 2001, highlighted the systemic flaws and inaccurate interpretations of existing law under which the nation's intelligence and law enforcement agencies operated and which restricted common-sense sharing of intelligence information among these agencies. In an effort to enhance counterterrorism authorities and remove these restrictions, the

Congress passed, and the President signed into law, the USA PATRIOT Act (Pub. L. No. 107–56) in October 2001.

The Act made modifications in several different areas of law, each designed to limit the ability of terrorists to conduct their operations and to secure the United States from further terrorist attacks. For example, Title II of the Act enhanced surveillance and information sharing authorities. Title IX addressed restrictions on asset recruiting for intelligence operations; required mandatory disclosure of foreign intelligence information acquired during the course of a criminal investigation to national security officials; and required the Attorney General and Director of Central Intelligence (DCI) to coordinate the training of law enforcement and other officials to identify and use foreign intelligence information in the course of their official duties. Sixteen of the Act's important provisions—as well as the recently enacted "lone wolf" amendment to the FISA (Intelligence Reform and Terrorism Prevention Act of 2004, Section 6001 (Pub. L. No. 108–458))—will expire on December 31, 2005.

Since enactment of the USA PATRIOT Act, the Committee has exercised careful oversight of the use and administration of the investigative tools authorized by the legislation. The Committee has held a series of hearings and received numerous briefings on the Intelligence Community's use of USA PATRIOT Act authorities. The Committee also has received detailed reports from the Department of Justice (DoJ) regarding FISA collection and the use of other surveillance tools. Moreover, the Committee is in the final stages of completing its second audit of the procedures, practices, and use of the FISA. This comprehensive, classified analysis will represent one of the most thorough reviews of Executive branch activities under the FISA since the USA PATRIOT Act was enacted.

The Committee notes that, in addition to its own oversight activities, three other Congressional committees with oversight responsibility have held at least 12 hearings this year regarding the USA PATRIOT Act. Since January 2005, a total of 20 witnesses from the DoJ, including the Attorney General, the Director of the Federal Bureau of Investigation (FBI), and the Deputy Attorney General, have testified before either this Committee, the House Permanent Select Committee on Intelligence, or the House and Senate Judiciary Committees on the reauthorization of the Act's expiring provisions and related matters. In addition, during the 108th Congress (the last period for which records were available at the time of this writing), the DoJ answered more than 520 Questions for the Record and responded to at least 100 letters from Members of Congress specifically addressing the USA PATRIOT Act.

The Committee is aware that a number of the Act's provisions have been characterized as being controversial. However, the reports of the DoJ Inspector General, the hearings of the Committee and its follow-up inquiries to the DoJ and the FBI, and the Committee's general oversight activities have revealed no instance in which a citizen's privacy rights or civil liberties have been violated by the use of authorities provided under the Act. Indeed, the record reflects that the DoJ's and the FBI's use of those authorities has been judicious and fully consistent with the law.

As a result of its extensive oversight activities, the Committee is convinced that the tools and authorities provided to the Intelligence

Community through the USA PATRIOT Act contribute significantly to international terrorism, espionage, and other foreign intelligence investigations. Failure to reauthorize those provisions that are set to expire will result in a return to the failed, outdated, and illogical limits on national security investigations that tied the hands of Intelligence Community and law enforcement officials prior to the terrorist attacks of September 11, 2001. Moreover, the Committee recognizes that national security investigators should have the same investigative tools provided to their counterparts investigating ordinary crimes. These additional, constitutional authorities are needed to effectively target terrorists and spies, particularly in time-sensitive investigations.

SECTION-BY-SECTION ANALYSIS AND EXPLANATION

The following is a section-by-section analysis and explanation of the legislation, as reported herein. Following the section-by-section analysis and explanation there are additional and minority views offered by Committee Members regarding this legislation and other matters.

TITLE I—REPEAL AND EXTENSION OF SUNSET ON CERTAIN AUTHORITIES

Section 101. Expansion of enhanced surveillance procedures not subject to sunset under USA PATRIOT Act

During the course of USA PATRIOT Act hearings and the staff audit of the FISA process, the Committee gathered information that overwhelmingly supports the permanent authorization of the intelligence and intelligence-related provisions in Title II of the USA PATRIOT Act, which are due to sunset on December 31, 2005. The Committee's review of these matters also disclosed the need for certain enhancements to existing authorities. These modifications are addressed in Title II of this legislation.

Section 101 permanently authorizes the intelligence and intelligence-related sections of the USA PATRIOT Act subject to the sunset deadline. Sixteen of the provisions in Title II of the Act are subject to sunset. Section 101 permanently authorizes the following nine provisions: 203(b) (authority to share electronic, wire, and oral interception information); 203(d) (authority to share foreign intelligence information); 204 (clarification of intelligence exceptions to criminal wiretap authorities); 206 (FISA "roving" authority); 207 (duration of FISA surveillance of non-U.S. persons who are agents of a foreign power), 214 (FISA pen register and trap and trace authority); 215 (FISA business records authority); 218 ("significant purpose"); and 225 (immunity for compliance with FISA wiretap). Each of these provisions is discussed in greater detail below. Because the remaining seven provisions are not directly connected to the intelligence and intelligence-related activities of the Government, the Committee has taken no action, or position, with respect to the remaining sections subject to the USA PATRIOT Act sunset provision.

Information Access

The information access provisions of Section 203 of the USA PATRIOT Act were lauded by the Executive branch during the Com-

mittee's hearings on the Act, and their utility was confirmed by the staff FISA audit. According to the witnesses, Section 203 has reduced the statutory and cultural barriers to information sharing that hindered national security investigations before September 11, 2001. The DoJ and the FBI informed the Committee that Section 203(b) has permitted disclosures of vital information to the Intelligence Community and national security officials on numerous occasions. They provided two specific examples in which intercepted communications in criminal cases contained foreign intelligence information. First, an investigation of a scheme to defraud donors and the Internal Revenue Service uncovered the illegal transfer of monies to Iraq and the manner and means by which those monies were transferred. Second, a sting operation in a money laundering investigation uncovered foreign intelligence information about an attempt to transport night-vision goggles, infrared lights, and other sensitive military equipment to a foreign terrorist organization.

The DoJ also provided a number of examples where intelligence information from a criminal investigation was appropriately shared with the Intelligence Community under 203(d). Some of these examples included ordinary domestic criminal investigations that discovered foreign intelligence information about violent terrorist training camps, plots to bomb soft targets abroad, an assassination plot, use of false travel documents, and logistical support networks for terrorist groups.

The Director of the Central Intelligence Agency also spoke approvingly of the information sharing procedures promulgated under Section 203. He cited the National Counterterrorism Center (NCTC) as one of the most positive illustrations of the current collaborative environment created by Section 203. He noted that NCTC receives foreign intelligence information obtained by the FBI during its criminal investigations. Such information is compiled with other foreign intelligence information and is used to produce all-source terrorism analysis that is disseminated throughout the Intelligence Community and to national security officials throughout the Government.

In a closed session, Intelligence Community officials provided specific examples of how the USA PATRIOT Act information sharing provisions were having a positive impact in ongoing classified investigations and operations.

All of the Executive branch witnesses stated that allowing Section 203(b) and (d) to expire would adversely impact currently robust information sharing relationships, discourage information access, and make it more difficult to detect and disrupt terrorist plots.

Finally, the staff FISA audit confirmed that the information sharing provisions in Section 203 have been successful, by all accounts. FBI agents in several field offices provided the audit staff with specific examples of cases in which they were able to use the USA PATRIOT Act information access provisions to neutralize targets in non-traditional ways.

Intelligence Exception to Criminal Electronic Surveillance Authorities

Section 204 provides an important exception for certain foreign intelligence activities from the requirements governing specified

criminal electronic surveillance activities. The Committee received no criticism regarding this provision, and it is imperative that the provision be made permanent.

FISA Multipoint or Roving Authority

A "multipoint" or "roving" wiretap order attaches to a particular surveillance target rather than to a particular phone or other communications facility. Prior to the enactment of Section 206 of the USA PATRIOT Act, such wiretaps, which have long been available in the criminal investigative context, were not available under the FISA.

Some commentators, though not opposed to the permanent authorization of the FISA roving authority granted in Section 206, have asked Congress to conform the FISA roving wiretap provision to the corresponding authority for roving wiretaps in the criminal code. Those commentators have suggested the addition of an "ascertainment" requirement that ensures law enforcement agents listen only to the conversations to which the target is a party. Others have proposed a requirement that the Government add additional specificity in its application for a FISA wiretap to more completely describe either the identity of the person whose phone or computer would be surveilled or the facility that would be tapped. In testimony before the Committee, some witnesses noted that their recommended changes are addressed in S. 737, the Security and Freedom Enhancement (SAFE) Act.

The SAFE Act contains a broad ascertainment requirement that would apply to any electronic surveillance where the facility or place at which the surveillance will be directed is not known at the time the order is issued. In such circumstances, the person conducting the surveillance could only initiate coverage when the presence of the target at a particular facility or place is ascertained. This would apply to all means of electronic surveillance. See Section 2, S. 737. By comparison, the criminal roving authority only requires ascertainment in the context of the interception of oral communications (e.g., by a microphone). See 18 U.S.C. 2518(12). The ascertainment requirements of the SAFE Act are not necessary in the FISA context because the Foreign Intelligence Surveillance Court (FISC) can fashion specialized minimization procedures depending upon the means by which the electronic surveillance is conducted. See 50 U.S.C. 1804(a)(11), 1805(c)(1)(F). When appropriate, the FISC has the authority to approve an ascertainment requirement designed specifically to collect primarily the target's communications and to limit the amount of incidental collection. Thus, there is no need to build the criminal ascertainment requirement for oral communications into the FISA, much less the extremely broad ascertainment requirement contained in the SAFE Act.

The SAFE Act also would require the FISC to specify either the identity of the target, or a description of the target and the nature and location of the facilities and places at which the electronic surveillance will be directed. In the context of roving electronic surveillance under the FISA, the Government already must provide the identity of the target, if known, the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known, and sufficient information so that the FISC

may find that the actions of the target of the application may have the effect of thwarting the electronic surveillance. See 50 U.S.C. 105(c)(1)(A)–(B), (C)(2)(B). In addition, the Government must establish probable cause that the target of the surveillance is a foreign power or an agent of a foreign power. See 50 U.S.C. 1805(a)(3). These four requirements together require a sufficiently adequate description of the target to ensure that the FISA roving authority is not used to broadly collect and retain the communications of innocent third parties.

In addition to these unclassified protections, the Committee has received classified information from the DoJ describing additional reasons an ascertainment requirement is not necessary in the context of FISA roving surveillance. The Committee will continue to closely examine the safeguards now in place, whether in law or practice, designed to prevent misuse of the FISA roving surveillance authority.

Duration of FISA Surveillance

Section 207 of the USA PATRIOT Act increased the maximum duration of FISA electronic surveillance and physical search orders under certain circumstances. Under Section 207 of the Act, initial surveillance and physical search orders directed against non-U.S. person members of international terrorist groups or officers or employees of foreign powers can be authorized up to 120 days (instead of 90 days) and renewed for up to one year (instead of 90 days). Section 207 also extended the duration of physical search orders directed against U.S. persons to 90 days (instead of 45 days) to match the standard duration period of an electronic surveillance order directed against a U.S. person.

Some critics of Section 207 have noted that the time periods for FISA orders are already much longer than for criminal surveillance orders. These critics have expressed concern that permitting surveillance to continue for a year with no judicial review opens the door for potential abuse. They have suggested that Congress should provide sufficient funds to the DoJ and the FISC to provide the necessary personnel and equipment to process FISA applications with shorter periods of duration.

Both the Executive branch witnesses and the staff FISA audit confirmed that Section 207 has been instrumental in allowing the FBI and the DoJ Office of Intelligence Policy and Review (OIPR) to conserve their limited resources to process FISA applications. By making the time periods for physical search and electronic surveillance equivalent, Section 207 has allowed the DoJ to file streamlined, combined electronic surveillance and physical search applications that, in the past, were tried but abandoned as too cumbersome to be effective. The DoJ further noted that if Section 207 were allowed to sunset, DoJ personnel would be forced to spend more time on routine extensions of current FISA orders and less time on applications relating to new targets. Also, DoJ personnel would have less time to oversee investigations involving the authorized surveillance of U.S. persons.

The staff FISA audit found that Section 207 has enabled the FBI and the OIPR to process more effectively certain non-U.S. person FISA applications. The audit revealed that the FISA process is still showing the strain from efforts to adjust to the post-9/11 oper-

ational environment, as evidenced by a significant number of initiation requests that were backlogged in the system. Therefore, the Committee has recommended permanent authorization of Section 207 of the USA PATRIOT Act, in addition to modification of other FISA time limits in Section 216 of this legislation.

FISA Pen Register and Trap and Trace Devices

Section 214 of the USA PATRIOT Act made the standard contained in the FISA for obtaining an order for a pen register or trap and trace device consistent with the standard for obtaining an order for a criminal pen register or trap and trace device (i.e., relevance to an ongoing investigation). Compare 50 U.S.C. 1842 with 18 U.S.C. 3123. Section 214 accomplished this by eliminating the FISA application requirement that the telephone line subject to the pen register or trap and trace device has been, or is about to be, used in communication with a foreign power or an agent of foreign power. Section 214 also incorporated an additional safeguard that such an investigation could not be conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

Some critics of Section 214 have asserted that the FISA pen register statute allows the FISC to act as little more than a "rubber stamp." Those critics have testified that the statute is silent on the need for a factual predicate in the underlying application. The SAFE Act would amend the FISA pen register statute to require a statement by the applicant of "specific and articulable facts" showing there is reason to believe that the information likely to be obtained is relevant to an ongoing national security investigation.

The "rubber stamp" criticism undervalues the FISC's authority to modify Government requests for FISA pen registers (see 50 U.S.C. 1842(d)(1)) and does not adequately account for current Government pleading practice before the FISC. The FISA pen register provision requires a certification that the information likely to be obtained is relevant to an ongoing national security investigation. See 50 U.S.C 1842(c)(2). Thus, the Government application must satisfy the FISC that the requested records are relevant to a lawful investigation. Otherwise, the FISC may deny the application or direct modification of the requested order. Therefore, the Government application must contain a sufficient explanation supporting the assertion that information sought is relevant to an ongoing, lawful investigation. Moreover, before an authorized national security investigation can be initiated, the FBI must meet the factual predicate required by the FISA, Executive Order 12333, and Attorney General implementing guidelines. The FBI is not authorized to investigate or maintain information on United States persons solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution. These statutory and regulatory safeguards prevent the FBI from engaging in random "fishing expeditions" to collect information on innocent U.S. persons. Thus, the additional requirements proposed in the SAFE Act are unnecessary.

In addition to the protections afforded by current law and practice, Section 217 of the legislation would require that a FISA application for a pen register or trap and trace order (or a FISA business records order) include "an explanation . . . that supports the assertion" that the information sought is relevant to a lawful inves-

tigation. This modification is designed to codify current Government pleading practice.

The FISA audit staff was informed that when a federal court issues an order for a criminal pen register or trap and trace device, the court has the authority under 18 U.S.C. 2703(d) to routinely require the service provider to supply subscriber information in its possession for the numbers or e-mail addresses captured by the devices. The FISA pen register/trap and trace provision has no comparable authority. Section 215 of this bill addresses this discrepancy.

FISA Business Record Orders

Section 215 of the USA PATRIOT Act made two important changes to the FISA "business records" authority. First, it broadened the scope of records that could be sought to "any tangible things," rather than the limited classes of records allowed by the then-existing version of the statute. Second, it allowed the FBI to make an application "for an investigation" to protect against international terrorism or clandestine intelligence activities. The DoJ has interpreted the "for an investigation" standard to be the practical equivalent of a "relevance" standard.

No witness before the Committee testified against permanent authorization of Section 215. Rather, some witnesses supported proposed SAFE Act amendments to the FISA business record provision. The SAFE Act would make a number of modifications to the FISA business records provision. First, it would raise the FISA business records standard from "for an investigation" to "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power." Second, it would modify the permanent nondisclosure period currently embodied in the FISA in favor of a nondisclosure period of 180 days that could be extended in 180-day increments only by an order of the FISC. Third, it would allow the recipient of a FISA order to consult with an attorney and those persons necessary to comply with the order. Fourth, it would permit the recipient to seek judicial review to modify or set aside the order. Fifth, it would place limitations on the dissemination and use of information obtained with a FISA order. Sixth, it would require that notice be provided to an "aggrieved person" when using the information in a trial or proceeding. Finally, it would provide procedures for making motions to suppress information obtained with a FISA order.

The Attorney General has supported clarifying the FISA to make the "relevance" standard explicit, to specifically permit consultation with an attorney under the FISA nondisclosure provision, and to allow a recipient to challenge a business records order before the FISC. The Attorney General, however, did not support the imposition of other limitations on FISA nondisclosure requirements. The Attorney General also testified that raising the FISA business record standard from "relevance" to "specific and articulable facts" would "make the use of [Section] 215 sort of a dead letter." The SAFE Act provisions which place limitations on dissemination and use of information obtained with a FISA business records order are very similar to the limitations in place for information acquired during the course of an electronic surveillance or physical search.

Also, the notice requirements and suppression procedures in the SAFE Act appear to be modeled on the procedures in place for electronic surveillance and physical search. These limitations, notice requirements, or suppression procedures, do not seem appropriate, given that requests for third party records are not nearly as invasive as the information obtained during a FISA electronic surveillance or physical search.

The Committee does believe, however, that certain modifications to the FISA business record authority are warranted. These modifications (such as an explicit "relevance" standard, tailored nondisclosure exemptions, judicial review procedures, and specific reporting requirements for certain types of records) are contained in Section 211 of this bill. In addition, Section 217 of the legislation codifies current Government pleading practice by requiring that a FISA business records application provide "an explanation . . . that supports the assertion" that the information sought is relevant to a lawful investigation.

FISA "Significant Purpose"

Section 218 of the USA PATRIOT Act is often credited as the provision that helped tear down the information sharing "walls" that had developed over the years prior to September 11, 2001, and separated intelligence agents from criminal agents and prosecutors. The original statutory text of the FISA required an official to certify that "the purpose" of the surveillance (or search) was to obtain foreign intelligence information. Section 218 amended that text to require a certification that "a significant purpose" of the surveillance (or search) is to obtain foreign intelligence information. This seemingly minor textual change set off a series of events that eventually led to the first, and only, decision by the Foreign Intelligence Surveillance Court of Review (Court of Review). See In re: *Sealed Case,* 310 F.3d 717 (U.S. FISCR 2002).

The reasoning of In re: *Sealed Case* provides a number of important insights into the FISA statute and process. First, the FISA, as passed by Congress in 1978, clearly did not preclude or limit the Government's use, or proposed use, of foreign intelligence information, which included evidence of certain kinds of criminal activity, in a criminal prosecution. See 310 F.3d at 727. The Court of Review reached this conclusion after conducting an in-depth review of the statute, legislative history, and relevant case law. See id. at 722–27. The Court of Review was puzzled that the DoJ, at some point during the 1980's, began to read the FISA as limiting its ability to obtain FISA orders if it intended to prosecute the targeted agents-even for foreign intelligence crimes. See id. at 723.

Second, although the original FISA did not contemplate a "false dichotomy" between intelligence and criminal investigations, the Court of Review opined that the USA PATRIOT Act's "significant purpose" and "consultation" amendments actually did—which had the ironic effect of making the "false dichotomy" true. See 310 F.3d at 735. In other words, Section 218 tore down an imaginary "wall" that never actually existed, and, in its place, created an actual distinction between foreign intelligence and law enforcement that had never existed in the FISA. This created an "analytic conundrum" for the Court of Review: had Congress accepted the dichotomy between intelligence and law enforcement by adopting the "signifi-

cant purpose" test without also amending the definition of the term "foreign intelligence information," which clearly includes evidence of foreign intelligence crimes? See id.

To resolve this "analytic conundrum," the Court of Review read the FISA statute to preclude the use of the FISA as a collection tool if the sole objective of such collection was criminal prosecution. In other words, so long as the Government entertains a realistic option of dealing with the target other than through criminal prosecution, it satisfies the "significant purpose" test. See 310 F.3d at 735. In its consideration of this issue, the Court of Review stated that the FISA process should not be used as a device to investigate ordinary crimes wholly unrelated to foreign intelligence crimes such as international terrorism, espionage, sabotage, and other hostile acts that threaten national security. However, the Court of Review recognized that sometimes even ordinary crimes might be inextricably intertwined with foreign intelligence crimes, such as when a terrorist engages in bank robberies to finance the manufacture of a bomb. See id. at 736.

To resolve whether a required non-prosecutorial purpose exists, the Court of Review clarified that the Government's purpose as set forth in a FISA application certification is to be judged by the national security official's articulation and not by a FISC inquiry into the origins of the investigation or an examination of the "types" of personnel involved. If the FISC has reason to doubt that the Government has any real non-prosecutorial purpose in seeking foreign intelligence information with a FISA surveillance or search, it can demand further inquiry into the certifying officer's purpose, or perhaps even the Attorney General's or Deputy Attorney General's reasons for approving the application. See 310 F.3d at 736.

This reasoning led the Court of Review to find that the FISC erred when it took portions of the Attorney General's augmented 1995 procedures—modified to incorporate the "significant purpose" standard in Section 218 of the USA PATRIOT Act—and imposed them generically as minimization procedures. See 310 F.3d at 730. The FISC's decision and order not only misinterpreted and misapplied minimization procedures it was entitled to impose, but may well have exceeded the constitutional bounds that restrict an Article III court when the FISC attempted to place limits and restrictions on the internal organization and investigative procedures of the DoJ. See id. at 731. The Court of Review also found that the FISC's refusal to consider the legal significance of the USA PATRIOT Act's crucial amendments was erroneous. See id. at 732. The practical impact of the Court of Review's decision was to remove the "walls" that had developed over the years that separated intelligence agents from criminal agents and prosecutors. Unfortunately, the Court of Review opinion could also be read to put in place a different kind of "wall"—one that actually exists.

As it relates to the historic discussion of the FISA statute and the approval of the Attorney General's augmented FISA procedures, the Committee explicitly endorses the Court of Review's decision. The Committee, however, is very concerned with one aspect of the opinion, and in Section 202 of this bill takes action to explicitly correct the potential negative ramifications of certain dicta in the Court of Review opinion. After finding that the USA PATRIOT Act's "significant purpose" and "consultation" amendments had the

ironic effect of creating a "false dichotomy" where none previously existed, the Court of Review stated:

> Of course if the [FISC] concluded that the government's sole objective was merely to gain evidence of past criminal conduct—even foreign intelligence crimes—to punish the agent rather than halt ongoing espionage or terrorist activity, the application should be denied.

310 F.3d at 735. This reasoning has been cited in subsequent decisions. See *American Civil Liberties Union* v. *U.S. Dep't of Justice,* 265 F.Supp. 2d 20, 32 n.12 (D.D.C. 2003), *United States* v. *Sattar,* 2003 WL 22137012, 12 (S.D.N.Y. 2003) (unpublished opinion). If permanent authorization of the "significant purpose" amendment in Section 218 of the USA PATRIOT Act would create a "false dichotomy" between foreign intelligence and law enforcement, the Committee cannot accept that outcome. Rather, the permanent authorization of Section 218 is intended to ensure that the "walls" are never rebuilt, and that the FISA may be used to gain evidence to prosecute targets for their past or future criminal conduct involving a "foreign intelligence crime," as that term was defined by the Court of Review in In re: *Sealed Case*. See 310 F.3d at 723. Simply put, evidence of a crime related to sabotage, international terrorism, clandestine intelligence activities, or other foreign intelligence crimes (including evidence of an ordinary crime "inextricably intertwined" with a foreign intelligence crime), is a wholly-included subset of the term "foreign intelligence information."

It is perfectly permissible under the FISA to conduct electronic surveillance or a physical search when the intent of the collection is the protection of national security by criminal prosecution of any foreign intelligence crime the target may have committed or intends to commit. Thus, if the Government intends to prosecute a suspected spy from the moment it begins its espionage investigation of the target, the Government may appropriately seek a FISA order. If a terrorist is engaging in cigarette smuggling to raise funds for a terrorist group, and the Government intends to prosecute the target for cigarette smuggling, the Government may appropriately seek a FISA order because such criminal activity is inextricably intertwined with a foreign intelligence crime. It would not be a permissible use of FISA surveillance or search authority, however, if the Government's sole purpose was the criminal prosecution of the target for an ordinary or non-foreign intelligence crime. Under such circumstances, the Government would have to seek a criminal search warrant or electronic surveillance order. Regardless, if the certifying official could certify that a significant purpose of the surveillance or physical search is to obtain foreign intelligence information about the target's international terrorism or clandestine intelligence activities, then any incidental collection of non-foreign intelligence criminal activity would be proper.

To further ensure that the "false dichotomy" is eliminated and the statutory question of purpose is resolved in favor of keeping any "walls" that may have existed from being rebuilt, Section 202 of this bill amends the FISA definition of "foreign intelligence information" to authorize the use of law enforcement methods, including prosecution, when so doing would protect against specified national security threats.

Civil Immunity

Section 225 of the USA PATRIOT Act may be one of the least controversial of the provisions subject to sunset. The provision provides immunity from civil liability to any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a FISA court order or request for emergency assistance under the FISA. The DoJ noted that this provision was modeled on the immunity provision which protects those persons or entities who assist the Government in carrying out criminal investigative wiretaps. See 18 U.S.C. 2511(2)(a)(ii). Section 225 is important because it helps secure the prompt cooperation of private parties with the Intelligence Community to ensure the effective implementation of FISA orders. The Committee received no criticism of Section 225 during its review of the FISA process and the USA PATRIOT Act provisions subject to sunset.

Section 102. Extension of sunset of treatment of individual terrorists as agents of foreign powers

Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004 amended the FISA by expanding the definition of an "agent of a foreign power" to include any person, other than a United States person, who "engages in international terrorism or activities in preparation therefor." This authority is sometimes referred to as the FISA "lone wolf" provision. Section 6001 is scheduled to sunset on December 31, 2005. The Attorney General and the Director of the FBI have both requested that this provision be made permanent. Section 102 of this bill extends the sunset on Section 6001 until December 31, 2009.

Since the FISA's enactment in 1978, the targets of intelligence collection and their means of communication have changed dramatically. Intelligence Community collection efforts are increasingly challenged by enhancements in communications technology and by the changing nature of intelligence targets. The FISA "lone wolf" provision permits the Government to apply for a FISA warrant to monitor a foreign person—i.e., not a citizen or lawful permanent resident of the United States—who is engaged in or preparing to commit acts of international terrorism, even if it is not known whether the foreign person is connected to an international terrorist group engaged in or preparing to commit similar acts. If the FISC grants a FISA order, the Government will be able to monitor the activities of the foreign person via electronic surveillance or physical searches, as authorized by the FISA. The provision takes better account of current operational realities without damaging important privacy interests of U.S. persons.

The Attorney General is required to report semiannually on the use of the FISA "lone wolf" provision. Since the Committee expects that this provision will be used infrequently, this reporting requirement will allow Congress to closely monitor the implementation of this provision. As the Committee has not yet received the initial report on this matter, it is appropriate to extend the sunset so that regular reporting can inform whether Congress should permanently authorize the provision.

TITLE II—FOREIGN INTELLIGENCE SURVEILLANCE MATTERS

Subtitle A—Definitional Matters

Section 201. Clarification of contents of communications for purposes of Foreign Intelligence Surveillance Act of 1978

Section 201 amends the definition of the term "contents" in the FISA to make it consistent with Supreme Court precedent and the definition of the same term in "Title III" (governing electronic surveillance in criminal investigations). Section 201 is based upon a finding and recommendation of the staff FISA audit concerning the fact that the FISA uses two different definitions for the term "contents." In the context of a FISA pen register or trap and trace device, the statute incorporates the definitions of the terms "pen register" and "trap and trace device" used in 18 U.S.C. 3127. In Section 3127, both the terms "pen register" and "trap and trace device" contain the term "contents" within their definitions. Section 3127(1) incorporates the definition of "contents" from 18 U.S.C. 2510. Section 2510(8) defines "contents" as follows: "when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." Thus, the term "contents" in the context of FISA pen register and trap and trace orders is identical to that used for criminal pen registers and trap and trace devices, as that "criminal" definition is incorporated by reference.

In the context of FISA electronic surveillance, however, the term "contents" differs from the Title III definition at 18 U.S.C. 2510(8). The FISA defines "contents" with respect to electronic surveillance as follows: "when used with respect to a communication, includes any information concerning the identity of the parties to such communications or the existence, substance, purport, or meaning of that communication." 50 U.S.C. 1801(n) (emphasis added). This language makes the FISA definition of contents considerably broader because it includes any information that would identify the parties to a communication or the mere existence of such communication. The Supreme Court has held that the installation and use of a pen register is not a search within the meaning of the Fourth Amendment, and hence no warrant is required. See *Smith* v. *Maryland*, 442 U.S. 735, 739–46 (1979). Thus, the FISA definition of contents is more restrictive than *Smith* v. *Maryland* because it includes the mere existence of, or identity of the parties to, a communication, even though the acquisition of that information would not be subject to the warrant requirement of the Fourth Amendment.

The FISA legislative history explains that the reason for the broad phrasing of the "contents" definition was to ensure that the scope of the FISA was sufficient to protect legitimate privacy interests and so that pen register and trap and trace devices would be included within the definition of "electronic surveillance." See H.R. Rep. No. 95–1283, at 67–68 (1978). In 1998, when Congress added a separate subtitle within the FISA to authorize the use of pen registers and trap and trace devices consistent with *Smith* v. *Maryland*, it chose to incorporate the Title III definition of "contents" into that subtitle rather than modify the existing FISA definition. The legislative history is silent on why Congress took this approach. See H.R. Rep. No. 105–780, at 32 (1998). Section 201 cor-

rects this longstanding inconsistency by conforming the FISA definition of "contents" to that used in Title III.

Section 202. Clarification of foreign intelligence information for purposes of Foreign Intelligence Surveillance Act of 1978

Section 202 amends the FISA definition of "foreign intelligence information" to clarify that the term includes information that relates to the ability of the United States to protect against certain threats to the national security, including protection through the use of law enforcement methods such as criminal prosecution. The intent of this amendment is to ensure that the information sharing "walls" cannot be rebuilt and to clarify that Congress does not accept or intend to create the "false dichotomy" discussed in dicta by the Court of Review in In re: *Sealed Case*, 310 F.3d at 735.

The misinterpretation and misapplication of the "primary purpose" test by the DoJ and the FISC in the decades preceding the Court of Review's decision had a very real and negative impact on the Intelligence Community's investigations, analyses, and operations. The Committee received testimony in all of its hearings that the bifurcation of national security investigations into their criminal and intelligence components prevented cooperation between intelligence and law enforcement officials engaged in investigations—even investigations of the same target and even though both groups were working to protect national security. The Committee also received testimony that the USA PATRIOT Act's removal of these information sharing "walls" subsequent to the Court of Review opinion has allowed the Intelligence Community to better coordinate its investigations, analyses, and operations.

The combined effect of Section 202's clarification of the definition of "foreign intelligence information" with the "significant purpose" and "consultation" amendments of the USA PATRIOT Act should leave no doubt that national security investigations are hybrid investigations with fully integrated intelligence and law enforcement components. See 50 U.S.C. 1804(a)(7)(B), 1806(k), and 1825(k). The FISA was designed, in part, to allow the Government to protect against the "foreign intelligence crimes" discussed by the Court of Review. See In re: *Sealed Case*, 310 F.3d at 723. The goal of Section 202 of this bill and Sections 218 and 504 of the USA PATRIOT Act is to ensure that the President is able to use all lawful means, including criminal prosecution, to prevent and neutralize threats to the national security. Simply put, Section 202 makes clear that collection of evidence via the FISA to protect national security through the prosecution of a crime related to sabotage, international terrorism, clandestine intelligence activities, or other foreign intelligence crimes (including evidence of an ordinary crime "inextricably intertwined" with a foreign intelligence crime), is an appropriate use of the FISA electronic surveillance and physical search authorities.

Subtitle B—Other Matters

Section 211. Access to business records for investigations under Foreign Intelligence Surveillance Act of 1978

Section 215 of the USA PATRIOT Act (the FISA "business records" amendment) has been one of the most maligned provisions

of that Act. This Committee received testimony during each of its three open hearings on the USA PATRIOT Act regarding the exercise/use of Section 215. All of the witnesses agreed that Section 215 should be reauthorized, but they differed as to the modifications that should be made to "improve" the provision. Section 211 of this bill incorporates six modifications to the FISA business records provision that the Committee has found reasonable to address concerns that have been raised. Section 217 of the legislation makes an additional modification to codify existing Government pleading practice before the FISC.

First, the Committee has clarified that "relevance" to an authorized investigation is the correct standard for issuing a FISA business records order, as opposed to the current, equivalent standard of "for an investigation."

Second, FISA Section 501(a) (50 U.S.C. 1861(a)) contains the following redundant provision: "provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." Nearly identical text follows in the very next subsection that defines "an investigation" to mean that it cannot "be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States." Compare 50 U.S.C. 1861(a)(1) with 50 U.S.C. 1861(a)(2)(B). Section 211 corrects this redundancy by deleting the first provision. The elimination of this redundancy does not affect the existing (and continuing) prohibition against the initiation or conduct of an investigation (or the application for a FISA business records order) solely based on activities of a U.S. person that are protected by the First Amendment. See 50 U.S.C. 1861(a)(2)(B).

Third, Section 211 provides additional categories of individuals to whom the existence of a given FISA business record order may be disclosed. The current statutory limitation prohibits the recipient of a FISA business records order from disclosing to any other person that the FBI has sought or obtained such an order. The statute provides one exception to this prohibition—disclosure may be made only to those persons necessary to comply with the order. Section 211 provides two additional exceptions to this general rule. Under Section 211, the recipient may disclose the existence of the order to: (1) those persons to whom such disclosure is necessary to comply with the order; (2) an attorney for purposes of seeking legal advice (including legal assistance necessary to initiate and litigate judicial review of the order); or (3) other persons designated by the Director of the FBI or the designee of the Director. Should it become necessary for the recipient to disclose the matter beyond the one attorney permitted, the recipient, or the initial attorney, may seek approval from the Director of the FBI or the Director's designee to expand disclosure to other attorneys, paralegals, or staff necessary to respond to the order.

Fourth, Section 211 requires the Attorney General to adopt minimization procedures governing the retention and dissemination of information acquired by the FBI through the FISA business records order process. These procedures will provide an additional safeguard to ensure that FISA business record orders, and the information obtained therefrom, are used appropriately.

Fifth, Section 211 provides an explicit process for challenging a FISA business records order before the FISC. Following receipt of a FISA business records order, but before the return date specified, the person charged with production under the order may seek to modify or set aside the order. During this period, the recipient may also seek to modify or set aside the nondisclosure requirements normally applicable to such an order. Although proceedings before the FISC will be closed to the public (subject to the right of an open hearing in a criminal proceeding), the Government must request that the FISC review classified or other sensitive information ex parte and in camera—such review is not automatic. In addition, applying a standard similar to that found in Section 106(f) of the FISA (governing the disclosure of information to an aggrieved person), the FISC may disclose information reviewed ex parte and in camera to the person challenging the FISA business record order, under appropriate security procedures and protective orders, only when such disclosure is necessary for the FISC to make an accurate determination to modify or set aside the order. Under Section 211, the FISC may modify or set aside a FISA business record order if compliance would be unreasonable or oppressive, the same standard applicable to a grand jury subpoena under Federal Rule of Criminal Procedure 17(c)(2). Section 211 also requires the FISC to adopt and publish procedures governing such challenges.

Sixth, Section 211 amends the FISA business record authority by adding new reporting requirements. In addition to the total number of FISA business record orders and the total number of such orders either granted, modified, or denied, Section 211 also requires that the semiannual report include specific details about business record orders that involve the production of any tangible things related to: libraries or bookstores; the purchase of a firearm; health information; or certain tax information. The Committee believes that this oversight mechanism is preferable to other legislative approaches that would create "safe havens" or "carve outs" for certain classes of records, particularly when the Constitution does not require disparate treatment for those classes of records.

Section 212. National security mail covers

The process by which national security investigators have obtained mail cover information has been governed by U.S. postal regulations for nearly 30 years. See 39 C.F.R. 233.3. The authority to use of mail covers for law enforcement purposes first appeared in the 1879 postal regulations. Section 212 statutorily authorizes the continued use of mail covers in national security investigations. A "mail cover" is the process by which the U.S. Postal Service furnishes to the FBI the information appearing on the face of an envelope addressed to a particular address: i.e., addressee, postmark, name and address of sender (if it appears), and class of mail. The actual mail is delivered to the addressee and only the letter-carrier's notation reaches the FBI. A mail cover does not include the contents of any "sealed mail," as defined in existing U.S. postal regulations (see 39 C.F.R. 233.3(c)(3)) and incorporated in Section 212. Although the Supreme Court has not directly addressed the constitutionality of mail covers (the Court has denied certiorari in cases involving the issue), lower courts have uniformly upheld mail covers as consistent with the requirements of the Fourth Amend-

ment. See *Vreeken* v. *Davis*, 718 F.2d 343 (10th Cir. 1983); *United States* v. *DePoli*, 628 F.2d 779 (2d Cir. 1980); *United States* v. *Huie*, 593 F.2d 14 (5th Cir. 1979); *United States* v. *Choate*, 576 F.2d 165 (9th Cir.), cert. denied, 439 U.S. 953 (1978).

In a letter dated November 19, 2004, the Attorney General formally requested that the Postmaster General make certain modifications to those portions of the U.S. postal regulation governing national security mail covers. Those modifications were not made. The Committee addresses the concerns raised by the Attorney General in the November 19 letter with Section 212.

First, the standard for obtaining a national security mail cover is too vague. For a national security mail cover, the requesting authority must specify the reasonable grounds to demonstrate the mail cover is "necessary to protect the national security." See 39 C.F.R. 233.3(e)(2)(i). This standard injects subjectivity where none is needed. Section 212 resolves this problem by making the standard for obtaining a national security mail cover one of "relevance" to an authorized investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities. This is the same relevance standard already in use for FISA pen register/trap and trace orders, FISA business record orders, "national security letters," and (under Section 213 of this legislation) FISA administrative subpoenas.

Second, the current approval level necessary to request a national security mail cover is too high. Under current regulation, requests for national security mail covers must be approved personally by the head of the law enforcement agency requesting the coverage or one designee at the agency's headquarters level. See 39 C.F.R. 233.3(g)(8). Conversely, requests for criminal mail covers need only be in writing and from any law enforcement agency. See 39 C.F.R. 233.3(e)(2). Section 212 resolves this problem by permitting mail cover requests to be made by the Director of the FBI, or a designee of the Director in a position not lower than Deputy Assistant Director at Bureau headquarters or Special Agent in Charge (including an "acting" Special Agent in Charge) in a Bureau field office. This delegation authority is consistent with the approval levels permitted in the context of "national security letters." See, e.g., 18 U.S.C. 2709(b).

Committee oversight has also revealed some longstanding issues with the manner in which national security mail covers are processed. Current regulations leave the decision on whether a mail cover should be issued or renewed to the discretion of the U.S. Postal Service. Over the years and on a number of occasions, the U.S. Postal Inspection Service has unilaterally decided to discontinue the use of the mail cover technique in certain FBI national security investigations. On some occasions, the FBI was asked to provide additional information justifying the continuance of the mail cover technique in these investigations. Section 212 resolves this issue by making U.S. Postal Service compliance with a properly formatted national security mail cover request compulsory. The Committee does not believe that it is appropriate for the U.S. Postal Service to substitute its judgment for that of the FBI in the context of national security investigations.

In addition to these investigative concerns, the Committee has included in Section 212 safeguards for privacy and civil liberties that do not exist in current regulations. These safeguards include regulating information collection, requiring minimization procedures, protecting against unauthorized disclosure of the requests, and ensuring Congressional oversight of the investigative technique. A new Section 702(e) of the FISA directs the Attorney General to adopt minimization procedures governing the retention and dissemination of any records received by the FBI in response to a mail cover request. A new Section 702(f) of the FISA permits the U.S. Postal Service to make reasonable disclosures of FBI national security mail cover requests to U.S. Postal Service personnel when necessary to ensure compliance with the FBI requests. Finally, a new Section 703 of the FISA requires the Attorney General to provide semiannual reports that keep Congress fully and currently informed of the quantity and uses of national security mail covers.

Section 212, in a technical modification, also removes from the FISA an "effective date" title (currently Title VII of the FISA). All matters addressed by the "effective date" provision have come to fruition, and this amendment will have no substantive effect on any current FISA operations or proceedings.

Section 213. Administrative subpoenas in national security investigations

Section 213 authorizes the FBI to issue administrative subpoenas to provide timely access to records that are relevant to authorized investigations to protect against international terrorism and espionage or to obtain foreign intelligence information not concerning United States persons.

Administrative Subpoenas: In General

To gain access to records that are relevant to law enforcement investigations of criminal activity, the DoJ and the FBI have long utilized grand jury subpoenas (Fed. R. Crim. P. 17) and more recently, with respect to particular crimes, administrative subpoenas (see, e.g., 18 U.S.C. 3486 (authorizing administrative subpoenas for, inter alia, criminal investigations of health care fraud and sexual exploitation or abuse of children); 21 U.S.C. 876 (authorizing administrative subpoenas in controlled substance investigations); 31 U.S.C. 3733 (authorizing administrative subpoenas to investigate false claims against the Government)). See Graham Hughes, "Administrative Subpoenas and the Grand Jury: Converging Streams of Criminal and Civil Compulsory Process," 47 Vand. L. Rev. 573 (1994). The grand jury subpoena and administrative subpoena are similar investigative tools, permitting access to information or testimony relevant to an investigation without the prior approval of a judge. A grand jury subpoena is issued by a federal prosecutor. See *Doe* v. *DiGenova*, 779 F.2d 74, 80 n.11 (D.C. Cir. 1985) ("[A] grand jury subpoena gets its name from the intended use of the . . . evidence, not from the source of its issuance."). Administrative subpoenas are issued by an authorized official of the investigating agency. Judicial review of both grand jury and administrative subpoenas occur after-the-fact, and only if the recipient challenges the subpoena in court.

The use of administrative subpoenas has been upheld by the Supreme Court. Federal courts have enforced administrative subpoenas so long as the documents requested are relevant to an authorized investigation and the issuance of the subpoena meets the "reasonableness" requirements of the Fourth Amendment. See, e.g., *United States* v. *LaSalle Nat'l Bank*, 437 U.S. 298, 313 (1978) (requiring that information sought be relevant to a lawfully authorized inquiry); *Oklahoma Press Publishing Co.* v. *Walling*, 327 U.S. 186, 209 (1946) (holding that the requirements of the Fourth Amendment are satisfied if an administrative subpoena seeks information relevant to an investigation authorized by Congress and is "reasonable" in scope); see also, e.g., *United States* v. *Powell*, 379 U.S. 48 (1964). A finding of "probable cause" is not necessary to support the issuance of an administrative subpoena because Executive branch agencies may utilize the subpoenas only when authorized by Congress to support a lawful investigation and only to procure information relevant to that authorized investigation. See *Oklahoma Press Publishing Co.*, 327 U.S. at 209; see also *Donovan* v. *Lone Steer, Inc.*, 464 U.S. 408 (1984).

Administrative subpoenas have been utilized by many departments and agencies of the Executive branch to implement and enforce regulatory policies. According to the DoJ Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities (May 13, 2002) (hereinafter, "Administrative Subpoena Report"), there are "approximately 335 existing administrative subpoena authorities held by various executive branch entities under current law." See Administrative Subpoena Report at 5. For example, the Inspector General Act of 1978 (5 U.S.C. App. 6(a)(4)) authorizes agency Inspectors General to issue judicially enforceable administrative subpoenas for certain information necessary for the performance of their functions (including investigations of possible criminal violations). Section 104(e) of the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA) (42 U.S.C. 9604(e)) authorizes administrative subpoenas to aid in the enforcement of environmental laws. The Secretary of Labor can issue an administrative subpoena to investigate, among other things, a violation, or potential violation, of the Employee Retirement and Income Security Act (ERISA) of 1974. See 29 U.S.C. 1134. The Federal Maritime Commission may issue administrative subpoenas to enforce the provisions of the Foreign Shipping Practices Act. See 46 U.S.C. App. 1710a. These are only a few of the administrative subpoenas authorized for "regulatory" investigations.

National security investigators have several different tools to obtain information relevant to terrorism, espionage, and other national security investigations; each of these tools suffers from inherent limitations, however. The primary tool utilized by the FBI to obtain information relevant to national security investigations is a "national security letter." Using "national security letters," the FBI may request certain communication service provider records (18 U.S.C. 2709), financial institution customer records (12 U.S.C. 3414); financial information, financial records, and consumer reports (50 U.S.C. 436); credit agency consumer records for counterterrorism investigations (15 U.S.C. 1681v); and certain financial information and consumer reports (15 U.S.C. 1681u). The

records requested through "national security letters" do not cover all categories of information that may be relevant to an international terrorism, espionage, or other national security investigation. Moreover, while compliance with these "national security letters" is mandatory, the letters lack an explicit enforcement mechanism. If a recipient chooses not to comply, the FBI has little, if any, recourse to enforce compliance. Although useful investigative tools, the effectiveness of "national security letters" is hindered by their limited reach and lack of an explicit judicial enforcement mechanism.

The FBI may also utilize a FISA business records order to access "any tangible things" relevant to an investigation to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities. See 50 U.S.C. 1861. Although the FISA business records order may be used to access "any tangible thing" and does not have the scope limitations associated with "national security letters," the FBI can obtain information with a FISA business records order only after an extensive application and approval process through the FBI, the DoJ, and the FISC. On the other hand, a federal prosecutor need only sign and issue a grand jury subpoena to obtain similar documents in criminal investigations, yet national security investigators have no similar investigative tool. In addition to bureaucratic inefficiencies that delayed for over two years the implementation of the amendments made to the FISA by Section 215 of the USA PATRIOT Act, the Committee has noted that the inability to quickly access records has limited the usefulness of the FISA business records order.

In a speech before the FBI Academy in Quantico, Virginia, on September 10, 2003—two years after the terrorist attacks of September 11, 2001—the President called on Congress to grant the FBI the authority to issue administrative subpoenas for terrorism investigations:

> Under current federal law, there are unreasonable obstacles to investigating and prosecuting terrorism, obstacles that don't exist when law enforcement officials are going after embezzlers or drug traffickers. For the sake of the American people, Congress should change the law, and give law enforcement officials the same tools they have to fight terror that they have to fight other crime.
>
> Here's some examples. Administrative subpoenas, which enable law enforcement officials to obtain certain records quickly, are critical to many investigations. They're used in a wide range of criminal and civil matters, including health care fraud and child abuse cases. Yet, incredibly enough, in terrorism cases, where speed is often of the essence, officials lack the authority to use administrative subpoenas. If we can use these subpoenas to catch crooked doctors, the Congress should allow law enforcement officials to use them in catching terrorists.

In an April 27, 2005, hearing before this Committee, both the Attorney General and the Director of the FBI reiterated the Administration's support for administrative subpoena authority to fight national security threats such as terrorism. DoJ officials have testi-

fied on several occasions before the Senate on the need for administrative subpoenas to support terrorism and other national security investigations. See *A Review of the Tools to Fight Terrorism Act*, 108th Cong., 2d Sess. (Sept. 13, 2004) (Joint Testimony of Daniel J. Bryant, Assistant Attorney General, Office of Legal Policy, U.S. Department of Justice, and Barry Sabin, Chief, Counterterrorism Section, Criminal Division, U.S. Department of Justice); *Tools to Fight Terrorism: Subpoena Authority and Pretrial Detention of Terrorists*, 108th Cong., 2d Sess. (June 22, 2004) (statement of Rachel Brand, Principal Deputy Assistant Attorney General, U.S. Department of Justice).

Authorized National Security Investigations

Section 213 provides the Attorney General with the administrative subpoena authority necessary to provide timely access to records or other materials that are relevant to authorized investigations to obtain foreign intelligence information not concerning U.S. persons or to protect against international terrorism and clandestine intelligence activities. The Attorney General may delegate the authority only to certain senior national security officials (a DoJ official with responsibilities for national security investigations not lower than an Assistant Attorney General, a United States Attorney, an Assistant United States Attorney with responsibility for national security investigations, the Director of the FBI, an FBI official not lower than a Deputy Assistant Director at Bureau headquarters, or a Special Agent in Charge (including an "acting" Special Agent in Charge) of an FBI field office). The administrative subpoena—a tool equivalent to the grand jury subpoena—may be used to further intelligence investigations of terrorists, spies, and other national security threats. The subpoena may be used only during the course of a lawful investigation authorized under the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (including the Executive Order 12333 limitation that foreign intelligence collection may not be undertaken for the purpose of acquiring information concerning the domestic activities of United States persons). Section 213 also expressly prohibits use of the administrative subpoena authority if an investigation of a United States person is based solely upon activities protected by the First Amendment. The administrative subpoena may not be used during the course of criminal investigations unrelated to international terrorism, clandestine intelligence activities, or the collection of foreign intelligence concerning non-United States persons. Any documentary evidence sought by the administrative subpoena will not be subject to disclosure if the information would be considered "privileged" if demanded by a subpoena duces tecum issued by a Federal court in aid of a grand jury investigation of espionage or international terrorism. A recipient that complies in good faith with an administrative subpoena under Section 213 is granted immunity from civil liability.

Nondisclosure Requirements

Although Section 213 provides authority to prohibit the disclosure of information concerning the issuance of the administrative subpoena, the nondisclosure requirements are not mandatory or automatic. To subject the administrative subpoena to limitations on

disclosure, the Attorney General or the issuing designee must certify that a danger to the national security may result from the public disclosure of the fact that a person has received a subpoena or that records were provided pursuant to such subpoena. If the nondisclosure requirements are applicable, a recipient may still disclose information concerning the subpoena to those persons to whom disclosure is necessary to comply with the subpoena, to an attorney for purposes of seeking legal advice (including legal assistance necessary to initiate and litigate judicial review of the subpoena), or to other persons designated by the Attorney General or the issuing designee. Should it become necessary for the recipient to disclose the matter beyond the one attorney permitted, the recipient, or the initial attorney, may seek approval from the Attorney General, or from the Attorney General's designee who issued the original administrative subpoena, to expand disclosure to other attorneys, paralegals, or staff necessary to resolve the matter.

If the Attorney General or the issuing designee determines that nondisclosure is no longer justified by a danger to national security, the recipient must be so notified. The requirement to examine the applicability of nondisclosure requirements under the statute is continuing. Issuing officials should monitor closely the status of the underlying investigation to ensure that disclosure would still result in a danger to national security. Nondisclosure requirements should not go stale because the need for such requirements has not been consistently and regularly examined. A formal review of the continuing applicability of nondisclosure requirements to issued subpoenas should occur at least every five years and be conducted by a senior official at the DoJ or the FBI.

During the course of a judicial review to modify or set aside an administrative subpoena, recipients may also challenge the applicability of nondisclosure requirements. If a recipient challenges the nondisclosure requirements, the Attorney General or the Director of the FBI must certify to the reviewing court that disclosure may still result in a danger to national security. The judicial review certification by the Attorney General or the Director of the FBI is not delegable.

Enforcement and Judicial Review

Section 213 is consistent with judicial precedent regarding the issuance of administrative subpoenas and provides protections for privacy and civil liberties through enforcement and judicial review procedures, mandated Attorney General guidelines governing use, and required Attorney General-approved minimization procedures.

Under Section 213, the Attorney General, or his designees, may issue an administrative subpoena only to obtain information relevant to a lawful, authorized investigation of specified matters. See *Oklahoma Press Publishing Co.*, 327 U.S. at 209. While the administrative subpoena may require the production of any records or materials and may require a certification by the custodian concerning the production of the records or other materials sought, the administrative subpoena cannot mandate testimony by any individual.

If a recipient refuses to comply with an administrative subpoena, the Attorney General may enforce the subpoena only through proceedings before a Federal district court or the FISC. A decision by

the DoJ to seek judicial enforcement of an administrative subpoena should not be made lightly. As the DoJ explained in the Administrative Subpoena Report:

> Where an agency requests the assistance of the Attorney General through the United States Attorney's office to seek enforcement of an administrative subpoena in federal district court, the United States Attorney's office plays a role that is more than ministerial, exercising discretion in determining whether to seek enforcement by a court. In evaluating such requests, the United States Attorney's office evaluates the subpoena issued by the agency to determine whether the scope of the request is in keeping with the agency's statutory authority and the agency has followed proper procedures in issuing the subpoena.

Administrative Subpoena Report at 10 (citing United States Attorneys Manual, 4–6.210 C). The Committee expects that this review, done in a timely fashion, will continue to play a crucial role in the proper and judicious use of administrative subpoenas under Section 213.

The judicial review provisions in Section 213 also provide an important check on the authority of the Executive branch. Under Section 213, any recipient of an administrative subpoena may challenge the issuance in a local Federal district court or before the FISC. As the Third Circuit noted in *Wearly* v. *FTC*, "the district court's role [in reviewing an administrative subpoena] is not that of a mere rubber stamp, but of an independent reviewing authority called upon to insure the integrity of the proceeding." *Wearly*, 616 F.2d 662, 665 (3rd Cir., 1980); see also *United States* v. *Security State Bank and Trust*, 473 F.2d 638, 641–42 (5th Cir. 1973) (noting that a statutory "system of judicial enforcement [provides] a meaningful day in court for one resisting an administrative subpoena"). Under Section 213, a court may modify or set aside an administrative subpoena if compliance would be unreasonable or oppressive, the same standard applicable to a grand jury subpoena under Federal Rule of Criminal Procedure 17(c)(2). Before setting an administrative subpoena aside and, thereby, depriving the Government of information needed to protect national security, the overriding role of the court should be modification of that subpoena to address any unreasonable or oppressive elements of the request.

Congressional Oversight and Reporting Obligations

The Committee will vigorously oversee and closely monitor the use of the administrative subpoena authority provided by Section 213. To support this oversight, Section 213 contains an extensive and detailed semiannual reporting requirement. The DoJ will be required to notify the Committee every six months regarding the number of administrative subpoenas issued, the total number of times a nondisclosure certification has been made, the number of judicial review proceedings initiated by recipients, the total number of administrative subpoenas modified or set aside by courts, and the total number of administrative subpoenas used to gain access to sensitive information from libraries or booksellers, information regarding the purchase of a firearm, health information, or certain tax information. The Committee will also closely monitor the imple-

menting guidelines issued by the Attorney General, in consultation with the Director of the FBI, and the minimization procedures approved by the Attorney General.

"National Security Letters" and FISA Business Records Orders

The Attorney General, in consultation with the Director of the FBI, is required to issue guidelines to implement the authority provided in Section 213 within six months of enactment of this legislation. Within six months of the issuance of such guidelines, the FBI must stop using certain specified investigative techniques—specifically, five "national security letter" authorities—in recognition of the similar authority provided in Section 213—and based on the additional protections for privacy and civil liberties expressly provided in Section 213. In addition, within one year of enactment, the Attorney General and the Director of National Intelligence must report to Congress regarding the continuing need for "national security letters" and FISA business records orders as investigative tools given the administrative subpoena authority provided by Section 213.

Sunset Provision

The administrative subpoena provision in Section 213 is subject to a sunset provision. On December 31, 2009, without further legislative action, the authority will expire. The sunset provision will give Congress the opportunity to revisit the manner in which the DoJ and the FBI have used the administrative subpoena authority established by Section 213, before Congress must act to authorize the investigative tool again.

Section 214. Modification of semiannual report requirement on activities under Foreign Intelligence Surveillance Act of 1978

Section 214 removes from Section 108(a)(2)(A) of the FISA (50 U.S.C. 1808(a)(2)(A)) a reporting requirement that is virtually impossible for the Attorney General to administer, because the FBI has significantly increased dissemination of foreign intelligence information to national security officials, including those in law enforcement positions. When the USA PATRIOT Act tore down the "walls" that prevented the sharing of FISA-derived foreign intelligence information with law enforcement officials (see discussion, supra, of Section 101 and 202), the Attorney General issued new procedures governing the minimization and dissemination of such information. These procedures, issued on March 6, 2002, "were designed to permit the complete exchange of information and advice between intelligence and law enforcement officials." See In re: *Sealed Case,* 310 F.3d at 729. These procedures were approved by the Court of Review on November 18, 2002. See id. at 746. Given Congressional intent to support increased information access and the judicially-approved Attorney General mandate to share FISA-derived foreign intelligence information, it is unreasonable to expect the Attorney General to continue attempts to comply with this reporting requirement. The Committee, however, maintains an existing FISA semiannual report that requires a description of "each criminal case in which information acquired under [FISA] has been authorized for use at trial during such reporting period." See 50

U.S.C. 1808(a)(2)(B). The Committee appreciates the specificity of current DoJ reporting of "each criminal case" in which FISA information has been authorized for use. The Committee expects that the current level of specific reporting will continue.

Section 215. Authority for disclosure of additional information in connection with orders for pen registers or trap and trace devices under Foreign Intelligence Surveillance Act of 1978

Section 215 authorizes the FISC to issue FISA pen register/trap and trace orders that also provide the Government subscriber information on the service targeted for surveillance and certain limited subscriber information associated with routing information captured by the surveillance devices.

During the staff FISA audit, the Committee found that FISA pen register/trap and trace orders were being underutilized for two reasons. First, FBI and DoJ bureaucratic delays in processing FISA pen register/trap and trace applications depress demand for the investigative tool. The FBI reported that it often takes as long to get a FISA pen register/trap and trace order as it does to get a "full content" FISA electronic surveillance order. By comparison, a criminal pen register/trap and trace order can usually be obtained on the same day it is requested. Second, FISA pen register/trap and trace orders are a less effective tool than the criminal law equivalent because—at least until fairly recently—investigators could obtain more information from the criminal pen register/trap and trace order. When a federal court issues a criminal pen register/trap and trace order, the court also has the authority under 18 U.S.C. 2703(d) to routinely require that the service provider furnish subscriber information for the captured numbers or e-mail addresses that are in its possession. The FISA pen register/trap and trace provision does not contain language that would permit the FISC to issue similar orders. Thus, the FBI is forced to use "national security letter" authority under 18 U.S.C. 2709 to obtain the same information. Unfortunately, the "national security letter" does not permit access to this customer/subscriber information in a timely fashion. The OIPR has found an intermediate solution to this problem by coupling a FISA business record order for subscriber records with a FISA pen register/trap and trace order.

Section 215 resolves this issue by authorizing the FISC to issue pen register/trap and trace orders that require a service provider to furnish certain subscriber information on the service targeted for surveillance and, if available, specified information concerning the subscriber accounts making incoming and outgoing communications on the targeted line. This provision is modeled on 18 U.S.C. 2703(c)(2) and (d).

Section 216. Surveillance of certain non-United States persons under Foreign Intelligence Surveillance Act of 1978.

Section 216 increases the maximum duration of a FISA electronic surveillance or physical search of a non-U.S. person agent of a foreign power who knowingly aids, abets, or conspires with any member of a group engaged in international terrorism. Under present law, such targets must be pled under the FISA "any person" standard and the duration of the initial search or surveillance cannot exceed 90 days and may only be renewed in 90-day increments. See

50 U.S.C. 1805(e) and 1824(d). This amendment would permit the Government to obtain initial electronic surveillance or physical search authority for 120 days on such non-U.S. persons, which then could be renewed for periods up to one year. This provision is a modest expansion of the improvements made by Section 207 of the USA PATRIOT Act, which increased the maximum duration of FISA electronic surveillance and physical search orders directed against non-U.S. person members of international terrorist groups or officers or employees of foreign powers.

Section 216 also increases the maximum duration of FISA orders for pen registers and trap and trace devices. Under present law, pen register/trap and trace orders can be initiated for a 90-day period and renewed only for an additional 90 days. Section 216 makes the order durations for a pen register/trap and trace device consistent with those for electronic surveillance and physical search. Thus, when an applicant certifies that the pen register/trap and trace device will likely obtain foreign intelligence information concerning a foreign power (as defined in paragraph (1), (2), or (3) of section 101(a)), the FISC may issue the first order for a period up to one year and authorize renewal periods of up to one year. When an applicant certifies that the pen register/trap and trace device will likely obtain foreign intelligence information concerning an agent of a foreign power (as defined in section 101(b)(1)(A)), the order may be initiated for up to 120 days and renewed for periods up to one year. All other FISA pen register/trap and trace orders may be initiated for up to 90 days and must still be renewed in 90-day increments.

The DoJ estimates that Section 207 of the USA PATRIOT Act has saved nearly 60,000 attorney hours. Put another way, Section 207 of that Act saved 30 lawyers a year's worth of work—and this estimate does not account for time saved by FBI agents, administrative staff, and the judiciary.

Section 216 would allow the DoJ and the FISC to focus more oversight scrutiny on applications for surveillance and physical search of U.S. persons. The section would also allow intelligence officials to spend more time investigating potential terrorist or espionage activity by non-U.S. persons, rather than wasting valuable time returning to the FISC to extend surveillance of foreign powers and agents of foreign powers that had already been authorized by the court.

Section 217. Additional information in applications for orders for pen registers and trap and trace devices and business records under Foreign Intelligence Surveillance Act of 1978

Section 217 codifies existing Government pleading practice before the FISC in applications for FISA pen register/trap and trace and business record orders. Some commentators have argued that Section 214 (pen register/trap and trace) and Section 215 (business records) of the USA PATRIOT Act deprive the FISC of discretion to deny a Government application for a FISA pen register/trap and trace or business record order. These commentators have expressed particular concern that the application requirements for FISA pen register/trap and trace and business record orders contain no required factual showing demonstrating how the information sought under such orders is relevant to a lawful investigation. Based on

the staff FISA audit and a review of FISA applications for pen register/trap and trace and business record orders, it is apparent that the Government currently provides in its applications a factual predicate for the FISC to make a determination of relevance. In order to codify existing practice, Section 217 amends the FISA to require that applications for both pen register/trap and trace and business record orders provide "an explanation . . . that supports the assertion of relevance" required by the FISA. The Committee does not expect this amendment to change current practice. The "explanation" requirement should not require additional information to support an application beyond the short and concise description already provided by the Government in such applications.

Section 218. Form of semiannual reports on access to business records under Foreign Intelligence Surveillance Act of 1978

Section 218 amends the reporting requirement in Section 502(b) of the FISA to encourage the submission of the report in unclassified form. The report may include a classified annex. The Committee encourages the Attorney General to include as much information as possible in the unclassified portions of this report, but recognizes that some information may provide information to terrorists, spies, and others that might threaten national security. The classified annex to this report should include any information the disclosure of which might threaten national security by providing information to the nation's enemies that would allow them to modify their activities to avoid detection.

Section 219. Report on voluntary disclosure of business records for Foreign Intelligence Purposes

Section 219 requires a one-time report from the Attorney General describing the policies and procedures applicable to the FBI's ability to request the voluntary disclosure of "tangible things" that are relevant to investigations to protect against international terrorism and espionage or to obtain foreign intelligence information not concerning United States persons. The FBI has a number of formal investigative tools to obtain information relevant to lawful national security investigations (e.g., "national security letters," FISA business records orders, grand jury subpoenas, and (under Section 213) administrative subpoenas). Often, however, a mere request for assistance is sufficient to gain access to information. Indeed, the assistance and awareness of the public has been termed the "first line of defense" against terrorism and other national security threats. Some have expressed concerns, however, that these "requests" might intimidate or coerce access to information that an individual otherwise may not have provided. The report required by this section is intended to provide a general overview of the FBI's practices and procedures relating to these "requests," including the "general frequency" of the requests and the "general frequency" that such requests are "denied." The Committee does not expect specific numbers of occasions if that information is not readily available, but instead hopes to gain a better understanding of this process. The report should be submitted in unclassified form, but may include a classified annex.

COMMITTEE ACTION

Motion to close

On May 26, 2005, on the motion of Chairman Roberts, by a vote of 9 ayes to 6 noes, the Committee voted to close the markup. The votes in person or by proxy were as follows: Chairman Roberts—aye; Senator Hatch—aye; Senator DeWine—aye; Senator Bond—aye; Senator Lott—aye; Senator Snowe—aye; Senator Hagel—aye; Senator Chambliss—aye; Vice Chairman Rockefeller—no; Senator Levin—no; Senator Feinstein—aye; Senator Wyden—no; Senator Bayh—no; Senator Mikulski—no; Senator Corzine—no.

Motion to report committee draft bill favorably subject to amendments

On May 26, 2005, on the motion of Chairman Roberts and by a vote of 8 ayes and 7 noes, the Committee voted to report the bill favorably, subject to amendment. The votes in person or by proxy were as follows: Chairman Roberts—aye; Senator Hatch—aye; Senator DeWine—aye; Senator Bond—aye; Senator Lott—aye; Senator Snowe—aye; Senator Hagel—aye; Senator Chambliss—aye; Vice Chairman Rockefeller—no; Senator Levin—no; Senator Feinstein—no; Senator Wyden—no; Senator Bayh—no; Senator Mikulski—no; Senator Corzine—no.

Amendments to committee draft bill

On May 26, 2005, by a vote of 8 noes and 7 ayes, the Committee rejected an amendment by Senator Feinstein to add in the section of the bill on administrative subpoenas a requirement and procedures to limit their use to emergency circumstances and to require Department of Justice review and approval before their issuance. The votes in person or by proxy were as follows: Chairman Roberts—no; Senator Hatch—no; Senator DeWine—no; Senator Bond—no; Senator Lott—no; Senator Snowe—no; Senator Hagel—no; Senator Chambliss—no; Vice Chairman Rockefeller—aye; Senator Levin—aye; Senator Feinstein—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Corzine—aye.

On May 26, 2005, by a unanimous vote of 15 ayes, the Committee agreed to an amendment by Chairman Roberts to add in the section of the bill on administrative subpoenas a modification to provide the authority to the Attorney General instead of the Director of the Federal Bureau of Investigation, to permit certain delegations of the authority, to make certain technical modifications regarding compliance with an administrative subpoena, to modify the procedures for consideration of classified information during the course of judicial review of an administrative subpoena, to require the Attorney General instead of the Director of the Federal Bureau of Investigation to issue implementing guidelines, to limit the ability of the Federal Bureau of Investigation to utilize "national security letters" six months after issuance of implementing guidelines, to require a report by the Attorney General and Director of National Intelligence on the continuing need for "national security letters" and for the authority provided by Title V of the Foreign Intelligence Surveillance Act of 1978 based on the authority to issue administrative subpoenas, and to subject the administrative subpoena authority to a "sunset" date of December 31, 2009, unless renewed.

The votes in person or by proxy were as follows: Chairman Roberts—aye; Senator Hatch—aye; Senator DeWine—aye; Senator Bond—aye; Senator Lott—aye; Senator Snowe—aye; Senator Hagel—aye; Senator Chambliss—aye; Vice Chairman Rockefeller—aye; Senator Levin—aye; Senator Feinstein—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Corzine—aye.

On June 7, 2005, by a vote of 8 noes and 7 ayes, the Committee rejected an amendment by Senator Feinstein to delete Section 203 (now Section 202) of the bill. The votes in person or by proxy were as follows: Chairman Roberts—no; Senator Hatch—no; Senator DeWine—no; Senator Bond—no; Senator Lott—no; Senator Snowe—no; Senator Hagel—no; Senator Chambliss—no; Vice Chairman Rockefeller—aye; Senator Levin—aye; Senator Feinstein—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Corzine—aye.

On June 7, 2005, by a vote of 8 noes and 7 ayes, the Committee rejected an amendment by Vice Chairman Rockefeller to modify Title V of the Foreign Intelligence Surveillance Act of 1978 to permit the Attorney General to require the production of business records under certain emergency situations without the approval of the Foreign Intelligence Surveillance Court, with a requirement that the request be presented to and approved by the Foreign Intelligence Surveillance Court as soon as practicable thereafter. The votes in person or by proxy were as follows: Chairman Roberts—no; Senator Hatch—no; Senator DeWine—no; Senator Bond—no; Senator Lott—no; Senator Snowe—no; Senator Hagel—no; Senator Chambliss—no; Vice Chairman Rockefeller—aye; Senator Levin—aye; Senator Feinstein—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Corzine—aye.

On June 7, 2005, by unanimous consent, the Committee adopted, on motion by Chairman Roberts, an amendment offered by Senator Levin to modify the standard of review applicable to the section of the bill concerning judicial review of administrative subpoenas. No Senator objected to this motion.

On June 7, 2005, by unanimous consent, the Committee adopted, on motion by Chairman Roberts, an amendment offered by Senator Levin to modify the records subject to disclosure pursuant to an administrative subpoena. No Senator objected to this motion.

On June 7, 2005, by a vote of 8 noes and 7 ayes, the Committee rejected an amendment by Senator Levin to modify the section of the bill on administrative subpoenas to require judicial review every 90 days of the decision to invoke the nondisclosure requirements applicable to administrative subpoenas. The votes in person or by proxy were as follows: Chairman Roberts—no; Senator Hatch—no; Senator DeWine—no; Senator Bond—no; Senator Lott—no; Senator Snowe—no; Senator Hagel—no; Senator Chambliss—no; Vice Chairman Rockefeller—aye; Senator Levin—aye; Senator Feinstein—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Corzine—aye.

On June 7, 2005, by a vote of 8 noes and 7 ayes, the Committee rejected an amendment by Senator Levin to modify a portion of Title I of the Foreign Intelligence Surveillance Act of 1978 governing electronic surveillance orders of the Foreign Intelligence Surveillance Court to require that, under certain circumstances,

such orders describe with sufficient specificity the target of the electronic surveillance. The votes in person or by proxy were as follows: Chairman Roberts—no; Senator Hatch—no; Senator DeWine—no; Senator Bond—no; Senator Lott—no; Senator Snowe—no; Senator Hagel—no; Senator Chambliss—no; Vice Chairman Rockefeller—aye; Senator Levin—aye; Senator Feinstein—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Corzine—aye.

On June 7, 2005, by a unanimous vote of 15 ayes, the Committee agreed to an amendment by Chairman Roberts, for himself and Vice Chairman Rockefeller, to modify Section 102 of the bill to extend for four years the "sunset" provision applicable to Section 6001 of the Intelligence Reform and Terrorism Prevention Act of 2004, to strike Section 201 of the bill in lieu of a modification to Section 216 of the bill, to add express procedures for judicial review before the Foreign Intelligence Surveillance Court of orders issued under Title V of the Foreign Intelligence Surveillance Act of 1978, to make certain technical modifications to Section 212 of the bill, to modify Section 216 of the bill to add a new category of "agents of foreign power" to the Foreign Intelligence Surveillance Act and to modify the time periods associated with pen register or trap and trace orders issued under Title IV of the Foreign Intelligence Surveillance Act, to add a new Section 217 to the bill modifying the application requirements for orders under Title IV and Title V of the Foreign Intelligence Surveillance Act, to add a new Section 218 to the bill relating to the form of semiannual reports under Title V of the Foreign Intelligence Surveillance Act, and to add a new Section 219 to the bill mandating a one-time report on voluntary disclosure of business records to the Federal Bureau of Investigation for foreign intelligence investigations. The votes in person or by proxy were as follows: Chairman Roberts—aye; Senator Hatch—aye; Senator DeWine—aye; Senator Bond—aye; Senator Lott—aye; Senator Snowe—aye; Senator Hagel—aye; Senator Chambliss—aye; Vice Chairman Rockefeller—aye; Senator Levin—aye; Senator Feinstein—aye; Senator Wyden—aye; Senator Bayh—aye; Senator Mikulski—aye; Senator Corzine—aye.

Motion to report bill favorably

On June 7, 2005, after disposition of all offered amendments, the Members of the Committee in person or by proxy recorded their final votes on reporting the bill favorably, 11 ayes and 4 noes, as follows: Chairman Roberts—aye; Senator Hatch—aye; Senator DeWine—aye; Senator Bond—aye; Senator Lott—aye; Senator Snowe—aye; Senator Hagel—aye; Senator Chambliss—aye; Vice Chairman Rockefeller—aye; Senator Levin—no; Senator Feinstein—no; Senator Wyden—no; Senator Bayh—aye; Senator Mikulski—aye; Senator Corzine—no.

ESTIMATE OF COSTS

Pursuant to paragraph 11(a)(3) of rule XXVI of the Standing Rules of the Senate, the Committee deems it impractical to include an estimate of the costs incurred in carrying out the provisions of this report due to the classified nature of the operations conducted pursuant to the legislation. On June 16, 2005, the Committee will transmit this bill to the Congressional Budget Office and request

that it conduct, to the extent practicable, an estimate of the costs incurred in carrying out the provisions of this bill.

EVALUATION OF REGULATORY IMPACT

In accordance with paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee finds that no substantial regulatory impact will be incurred by implementing the provisions of this legislation.

CHANGES IN EXISTING LAWS

In the opinion of the Committee, it is necessary to dispense with the requirements of paragraph 12 of rule XXVI of the Standing Rules of the Senate in order to expedite the business of the Senate.

ADDITIONAL VIEWS OF SENATORS ROBERTS, HATCH, DEWINE, BOND, LOTT, AND CHAMBLISS

Congress enacted the USA PATRIOT Act to correct the flaws in, and the interpretations of, U.S. law that prevented cooperation and information sharing between our intelligence and law enforcement agencies prior to the September 11 attacks. Because of the Act, we have seen significant progress in some areas. For that reason alone, the intelligence provisions of the Act, set to expire at the end of this year, should be permanently authorized. The Intelligence Committee's oversight activities have revealed, however, the need for additional legislation to ensure national security investigators have the tools they need to combat international terrorism and espionage. With this bill, the Committee would not only reauthorize the expiring provisions, but also provide the additional tools these investigators need.

We recognize that the USA PATRIOT Act has been the source of considerable controversy, and, as a result, some have questioned the need for permanently authorizing the legislation. But, the threats to our nation from terrorists and spies are not going to expire at the end of the year. The stakes are simply too high to return to the failed policies and procedures that tied the hands of our law enforcement and intelligence agencies before September 11.

Additionally, we now have had nearly four years of congressional oversight of the use of the tools provided by the USA PATRIOT Act. Despite rhetoric to the contrary, our oversight has revealed not a single substantiated incident of abuse of the authorities provided by the Act.

Our experience with the Foreign Intelligence Surveillance Act (FISA) business record provision highlights this point. This provision is often characterized as giving federal agents the authority to investigate the reading habits of innocent citizens through the seizure of library records. First of all, we should all remember that several of the 9–11 hijackers used library internet access to purchase and track the airline reservations they used to board the flights that they would soon hijack. The Federal Bureau of Investigation (FBI) should be able to access these library records using every constitutional tool available so—should the need arise—they might be able to prevent a future attack. Beyond that, we know through Congressional oversight that the FBI has used this authority only 35 times and never to access library records.

Given the FBI's careful and judicious use of the USA PATRIOT Act authorities provided after the September 11 attacks, Americans can be confident that any further grants of legitimate, constitutional investigative tools to national security investigators will be used only to protect Americans—not to deprive them of their privacy or civil liberties.

The bill reported by this Committee reflects a balanced approach to providing investigative tools to national security investigators while maintaining the checks and balances necessary to preserve civil liberties. First, the legislation permanently authorizes the nine intelligence-related provisions set to expire at the end of the year. Second, it extends to national security investigators tools already used in federal criminal cases. Third, it addresses concerns expressed by the critics of the USA PATRIOT Act by expressly establishing standards for the use of certain tools and increasing Congress's ability to oversee the use of every investigative tool it authorizes.

As with the USA PATRIOT Act, portions of the Committee's bill have been (and no doubt will continue to be) significantly mischaracterized. As discussed in greater detail below, many of the mischaracterizations of the bill's provisions are based on a misreading of the plain language of the bill and its accompanying report; a lack of understanding of—or a refusal to recognize—the safeguards and limitations imposed by statute, executive order, and agency regulations; and a flawed understanding of the role of the FBI in national security investigations.

ADMINISTRATIVE SUBPOENAS

Administrative subpoenas are well-established and constitutional investigative tools that Executive branch agencies have long utilized in criminal and regulatory investigations. In fact, Congress has legislatively authorized 335 different types of administrative subpoenas. The Attorney General currently uses administrative subpoenas to investigate drug trafficking, child pornography, health care fraud, and other crimes. Under current law, however, the Attorney General cannot use administrative subpoenas to investigate international terrorism or espionage. Section 213 remedies this deficiency by authorizing the Attorney General to issue administrative subpoenas to access records relevant to authorized investigations to protect against international terrorism and espionage or to obtain foreign intelligence information concerning non-U.S. persons.

Opponents of the administrative subpoena authority provided in Section 213 charge that the authority will allow federal agents unfettered discretion to conduct "fishing expeditions." The plain language of the provision and existing safeguards will prevent such abuse. The statute clearly restricts usage of administrative subpoenas to international terrorism, espionage, and certain other national security investigations. Thus, the authority under Section 213 may not be used for ordinary criminal investigations. Additionally, these investigations must be authorized under Executive Order 12333 (which places express limitations on the collection of information concerning the domestic activities of U.S. persons) and be consistent with guidelines issued by the Attorney General.

We are not granting this authority to the FBI of the 1960's, which was nearly devoid of congressional oversight. In contrast to its overreaching in the past, today's FBI honors the rule of law, is bound by executive order and Attorney General guidelines, and is subject to the vigorous oversight of Senate and House Intelligence Committees. Congress will monitor closely the FBI's use of admin-

istrative subpoenas and other USA PATRIOT Act authorities and will ensure that those authorities are not used for "fishing expeditions."

Opponents of the administrative subpoena provision also argue that, if administrative subpoena authority is granted to the Attorney General, its use should be restricted to instances in which there is an "emergency need" for the records or materials sought. Such a restriction would impose limits on national security investigators that Congress has not imposed on other regulatory or criminal investigators. In fact, of the 335 administrative subpoenas enacted by Congress, only one contains anything like an emergency circumstances requirement—the Secret Service administrative subpoena—and the requirements of the Secret Service provision are light compared to those proposed in an amendment offered by opponents of the Committee's administrative subpoena authority.

Other administrative subpoenas, like those authorized for criminal health care fraud, child pornography, and narcotics trafficking, contain no "emergency circumstances" requirement. If the Attorney General, or his designee, can issue an administrative subpoena without a finding of emergency circumstances to investigate a "dirty doctor," we see no reason to impose that burden on the investigation of a "dirty bomber."

Some opponents argue that the FBI's need for timely access to records and materials can be met simply by amending the FISA business records provision to allow the Attorney General to issue, without FISA court approval, an "emergency" order for production of business records or other tangible things. Like the proposals to limit administrative subpoenas to emergency situations, the proposals for emergency FISA business record orders contain burdensome administrative hurdles that are not required by the Constitution and will make the "emergency" business record order virtually useless.

Requiring national security investigators to get an Attorney General certification or to provide pre-issuance notification to the Foreign Intelligence Surveillance Court (FISC) places hurdles in front of these investigators that their counterparts in regulatory and criminal investigations do not face. These hurdles would essentially deprive any utility that the emergency order process might have granted. Additionally, early in an investigation the FBI might not have the information necessary to request emergency certification for a FISA business record order, not to mention the ability to quickly work that request through the internal FBI and Department of Justice (DoJ) review process all the way up to the Attorney General for approval.

Moreover, based on what we already know about the FBI's use of FISA business record orders, we question whether Attorney General "emergency certification" would ever be sought. As mentioned above, the FBI is using the FISA business records order in only a very small number of cases—35 times in nearly four years. This limited usage tells me that the bureaucracy already limits the effectiveness of the FISA business records tool. There is no reason to think a tool permitting Attorney General emergency authorization would be any more effective.

The bottom line is that in the two years of public debate on administrative subpoenas, we have not heard a compelling argument why Congress should not give national security investigators the same kind of tool we give criminal and regulatory investigators. We cannot hold the FBI responsible for failures to preempt terrorism and espionage if we fail to give them every available tool permitted by our Constitution. National security investigators should not be hamstrung by "emergency circumstances" requirements or be forced to use an inadequate substitute such as an emergency FISA business records order.

SECTION 202

Section 202 seems complex and difficult to understand. Don't be fooled. It simply amends the definition of "foreign intelligence information" under the FISA to clarify that the definition includes information that is necessary to the use of law enforcement methods, such as criminal prosecution, to protect against certain, specified crimes—international terrorism, sabotage, clandestine intelligence activities, and other "grave hostile acts"—when committed by foreign powers and agents of foreign powers. The Committee included this provision to ensure that the Foreign Intelligence Surveillance Court of Review (Court of Review) opinion (In re: *Sealed Case*, 310 F.3d 717 (U.S. FISCR 2002)) does not prevent the use of the FISA to collect evidence for the arrest and prosecution of an individual when his crimes are inextricably intertwined with foreign intelligence crimes. Even so, such law enforcement-type use of the FISA would only be appropriate when the prosecution of the target would protect against international terrorism, sabotage, espionage, and "grave hostile" threats.

Opponents of Section 202 claim that the provision will allow the FBI to use the FISA to collect intelligence solely for use as evidence in the prosecution of ordinary criminal acts. This argument is based on a misreading of the statute and accompanying report. First, even with the adoption of Section 202, the FISA could only be used against foreign powers or their agents engaged in foreign intelligence crimes or activities in preparation for such crimes. Second, Section 202 has been carefully drafted—along with its accompanying legislative history—to ensure that FISA "foreign intelligence information" only includes foreign intelligence crimes and other crimes "inextricably intertwined" with those foreign intelligence crimes. For criminal prosecutions in cases involving ordinary crimes, the Government would still have to seek a criminal search warrant or a criminal electronic surveillance order. These limitations prevent the Government from using the FISA solely for the purpose of criminal prosecution of ordinary crimes.

Opponents also claim that Section 202 "undermin[es] the distinction between intelligence and law enforcement" activities allegedly contained in the FISA. This argument, however, ignores the history of the FISA. Congress never intended that the FISA should contain a distinction between intelligence and law enforcement activities with regard to foreign intelligence crimes. When the FISA was passed in 1978, Congress made clear in the statutory language that the Government could use foreign intelligence information in criminal prosecutions. The distinction between intelligence and law en-

forcement activities grew out of improper interpretation and application of the FISA by the DoJ and the FISC.

The USA PATRIOT Act's "significant purpose" amendment to the FISA certification requirement was meant to tear down the "wall" between foreign intelligence and criminal law enforcement activities. It was an important amendment that rejected the old DoJ and FISC interpretations that created the "wall" and started the cultural change necessary to encourage cooperation between intelligence and law enforcement. That amendment, however, did not restore the balance Congress had originally set in 1978. The Court of Review interpreted the "significant purpose" amendment as potentially preventing the use of FISA information to prosecute international terrorists or spies for those and related crimes. In other words, the Court of Review interpreted the amendment as another potential "wall." Section 202 removes this possibility by clearly stating that the FISA can be used when the information collected is intended to be used for law enforcement measures that will protect the United States from international terrorism, sabotage, clandestine intelligence activities, and other grave hostile acts. Thus, rather than fundamentally changing the law governing FISA investigations, Section 202 actually restores Congress's original intent in adopting the FISA and the "significant purpose" amendment.

Finally, opponents claim that Section 202 threatens "to create uncertainty in the currently well-established relationship between intelligence and criminal proceedings" and argue that the provision should be deleted from the Committee's bill because the DoJ has not asked for the provision. This argument simply ignores the fact that the Court of Review itself pointed out that the "significant purpose" language creates a "false dichotomy" between intelligence and criminal investigations. Moreover, two district courts have already cited the Court of Review's reasoning on this issue. When a problem like this arises, Congress doesn't have to wait for the DoJ to request legislation before it acts. As Professor Richard Seamon pointed out to the Committee in his letter on this provision, "The Department [of Justice] has been wrong about this sort of thing before (having participated in building the wall)." Based on the fact that the courts are already relying on the reasoning of the Court of Review and given the DoJ role in erecting the original "wall" between intelligence and law enforcement investigators, Congress should act now to eliminate the risk that interpretations of the FISA will work to the benefit of international terrorists, spies, and others who would threaten our security.

SUNSETS

During markup of this legislation, the Committee voted to "sunset" two of the authorities provided in the bill. Specifically, the FISA "lone wolf" and administrative subpoena authority would cease to have effect on December 31, 2009, unless reauthorized. We are generally opposed to sunsets and do not believe that such restrictions are necessary in these cases. "Sunset" provisions discount or ignore Congress's role in overseeing the use of Executive branch authorities. Through normal oversight activities, the Congress is able to monitor the use of these authorities and, when required, make any necessary changes or modifications. By imposing sunsets,

Congress also implies that these authorities are somehow unique and, thus, require special protections. This is not the case. As discussed above, the administrative subpoena provision simply extends to the national security arena a tool commonly used in criminal and regulatory investigations. The "lone wolf" provision merely allows the use of FISA physical search and electronic surveillance tools in cases in which the Government knows the target of the search or surveillance is a non-U.S. person engaged in international terrorism activities, but is doing so on his own or in cases where the Government is unable to identify for whom the individual is working. These provisions provide common-sense authorities that help protect Americans. We fully expect to be reauthorizing these important authorities in four years.

CONCLUSION

When considering the Committee's bill, it is imperative to keep in mind that we are dealing with the Federal Government's ability to fulfill its primary obligation—protecting our nation from attack and preserving our way of life. Failure to reauthorize the expiring intelligence-related provisions of the USA PATRIOT Act will likely result in a return to the failed practices in place prior to the September 11 attacks. Hopefully, Congress will do its duty and permanently authorize these critical provisions. In going beyond reauthorization, however, the Committee has presented the Congress with a reasonable approach that further ensures our security by extending to national security investigators the constitutional tools currently available to their criminal counterparts while also preserving the checks and balances necessary for the protection of privacy and civil liberties.

PAT ROBERTS.
ORRIN G. HATCH.
MIKE DEWINE.
CHRISTOPHER S. BOND.
TRENT LOTT.
SAXBY CHAMBLISS.

ADDITIONAL AND MINORITY VIEWS OF SENATORS ROCKEFELLER, LEVIN, FEINSTEIN, WYDEN, BAYH, MIKULSKI, AND CORZINE

The primary task of the Congress this year, with respect to investigatory powers in national security investigations, is action on renewal of sixteen USA PATRIOT Act authorities that are scheduled to sunset, or expire, at the end of this year. The accompanying task is to correct any defects in or otherwise improve these provisions.

Sections 101 and 102 of the Committee bill would make permanent nine PATRIOT Act authorities (the others are within the sole jurisdiction of the Committee on the Judiciary), while also extending a sunset in the recently enacted Intelligence Reform Act for so-called "lone wolf" surveillance authority. In extending that sunset, the Committee accepted a proposal advocated by Senator Corzine that the Department of Justice should gain further experience under this new authority before Congress determines whether to make it permanent.

Section 211 of the Committee bill—by remedying some of the problems with Section 215 of the PATRIOT Act pertaining to orders by the Foreign Intelligence Surveillance Court for business records—is a step in the right direction toward accomplishing the second task. Also, Section 216 of the Committee bill, by increasing the maximum duration of certain Foreign Intelligence Surveillance Court orders, improves the FISA process by enabling Department of Justice personnel and the FISA Court to devote attention to new applications and other urgent matters.

However, the Committee bill goes beyond these core tasks. Notably, it adds a wide-ranging "administrative subpoena" to the Attorney General's and the FBI's broad powers in national security investigations. This significant new investigative authority and other proposed additions or changes to present law, as these additional views explain, are problematic and may even be damaging to our national security protections.

1. ADMINISTRATIVE SUBPOENAS

The bill proposes to add a new title to FISA to authorize the issuance of administrative subpoenas for production of records. The expressed justification for administrative subpoenas—which would not be reviewed by a court unless challenged by the recipient of the subpoena or if there is an enforcement action—is that they may be needed in emergency circumstances when alternative means for obtaining information might result in unacceptable delay.

Congress has granted subpoena authority to many agencies that exercise economic or other regulatory powers. Several enactments, in recent years, have provided subpoena authority to the Attorney General in controlled substances, health fraud, and child pornog-

raphy cases, and to the Secretary of the Treasury in matters involving imminent threats to persons protected by the Secret Service. Three of these measures, collected in 18 U.S.C. § 3486, contain important checks on the Government's use of that authority. None is as potentially vast in scope as the proposal to make this power available in national security investigations. Moreover, in none of these other matters had Congress already provided for an array of other powers, as it has done for intelligence investigations, including for a special court—the Foreign Intelligence Surveillance Court—whose sole mission concerns the grant of investigative powers.

When testifying before the Committee, the FBI could not document significant past or current instances when national security investigations faltered or were hindered due to lack of an administrative subpoena authority. The FBI argued that such a circumstance could exist in the future when immediacy might dictate moving quickly with a subpoena for records without prior judicial review. This may be true, but based on both demonstrated and anticipated need, the use of any such authority without prior review should be the exception, not the rule.

Notwithstanding the desire of the Administration for additional authority, the responsibility of Congress is to determine if there is a convincing need that justifies departure from the careful methodology of the Foreign Intelligence Surveillance Act. As part of that assessment, Congress should consider whether any such need is not met by the array of other authorities now available for obtaining business records in national security investigations, including through National Security Letters and grand jury subpoenas. If there is such a need, particularly a need that goes beyond emergencies, it has not been demonstrated in the legislative record presented to the Committee by the Department of Justice or established by the Committee's own factual inquiry. On the present record, all that Congress has is the Administration's wish for more.

By one vote, the Committee rejected an amendment by Senator Feinstein (set forth in the appendix to these views) to limit administrative subpoena authority to emergency use. It would have authorized administrative subpoenas upon the certification of the Attorney General or FBI Director, or their designees, that (1) it is impracticable to obtain in a timely fashion, by an order of the FISA Court or other means, the records or materials required and (2) there is a reasonable belief that there is an emergency need for the records or materials in order to protect against terrorism. The amendment would also have required approval from a U.S. Attorney or an Assistant Attorney General prior to issuance of an administrative subpoena, rather than at the sole discretion of an FBI Special Agent in Charge. To facilitate rapid action, approval could be oral as long as it is reduced to writing as soon as possible. The Feinstein amendment would tailor administrative subpoena authority to the need presented by the Administration: the occasional emergency when it is impractical to obtain a FISA Court order or other enforceable demand such as a grand jury subpoena.

In our view, absent an emergency, maintaining pre-issuance judicial review of requests for orders to produce business records is an important check against potential abuse in the investigative proc-

ess. The Administration acknowledges that the FISA Court has worked well and efficiently in reviewing subpoena requests. Unless changed, the bill effectively puts the court out of business with respect to business records, and puts the current subpoena authority of the court in the hands of the investigators. This is not necessary, justified, or wise.

The Committee also rejected by a one-vote margin an amendment by Senator Levin (also set forth in the appendix to these views) to establish a procedure to assess the continuing need, in individual cases, for nondisclosure requirements. The Committee's bill provides that disclosure of the receipt of an administrative subpoena—other than to persons necessary to carry out production of records, an attorney, or other persons as permitted by the FBI—is prohibited if the Attorney General or a designee certifies that a danger to national security may result. The bill also provides for criminal penalties for knowing violation of this prohibition. The length of the ban is not limited. It could prevent the recipient of a subpoena from exercising First Amendment rights to protest government action, including by bringing abuses to the attention of members of Congress or Inspectors General.

We recognize the importance of requiring nondisclosure in some cases, but any such requirement should be subject to judicial review. Senator Levin's amendment would have provided for periodic review of the nondisclosure requirement, enabling the FBI to extend the nondisclosure ban for repeated 90 day periods upon a showing to a court that a danger to national security may result. A similar provision exists in current law on criminal administrative subpoenas, 18 U.S.C. § 3486, which provides that nondisclosure orders issued by district courts last for ninety days subject to renewal.

While the appropriate length of time between the review of orders is open to discussion, the essential point of the amendment, which we strongly support, is that the combination of factors in the Committee's bill—a limitation on speech that is potentially for life and enforced by criminal penalties—makes it imperative that there at least be periodic court review of the requirement that a citizen or company remain silent about the receipt of a governmental subpoena.

2. SECTION 215 OF THE PATRIOT ACT

The ability of intelligence as well as law enforcement investigators to obtain relevant records expeditiously is critical. They may provide information that enables investigators to pinpoint more exactly what additional investigatory tools are necessary. Legally enforceable demands for records—whether they be called orders or subpoenas—also allow investigators to obtain information in a manner that is less intrusive than electronic surveillance or physical searches.

Section 215 of the PATRIOT Act (which amended Title V of the Foreign Intelligence Surveillance Act) significantly expanded the Government's ability to obtain "tangible things," including records, in international terrorism and other national security investigations. In doing so, the broad reach of Section 215 has prompted a

great deal of concern about the potential overreaching of Government demands.

The amendments reported by the Committee address some key concerns about Title V, as amended by Section 215. First, the amendments make explicit that the Government's application to the Foreign Intelligence Surveillance Court, for an order to obtain business records or other tangible things, must be for items that are "relevant" to a foreign intelligence investigation. Bolstering that requirement, the Committee's bill also provides, as advocated by Senator Wyden, that the application to the court "shall include an explanation by the applicant that supports the assertion of relevance."

The Committee's bill addresses one aspect of the nondisclosure regime established by Title V of FISA. As amended in 2001 by Section 215 of the PATRIOT Act, Title V provides that no person shall disclose to any other person, other than persons necessary to produce the things required by an order, that the FBI has sought or obtained things under the section. The Attorney General told the Committee that he supports a clarification in Title V that permits disclosure to an attorney. The bill, accordingly, makes clear that the recipient of an order for production of records may disclose the order to an attorney to obtain legal advice or assistance.

While no amendment was offered in Committee to address other aspects of Title V's nondisclosure requirement, the reasons warranting periodic review of the related nondisclosure requirement for administrative subpoenas also apply to Title V and merit the attention of Congress as it considers amendments to that title.

In accord with the Attorney General's further representation to the Committee, the bill also provides explicitly for judicial review. Following receipt of an order to produce, but before production, the recipient of the order may petition the Foreign Intelligence Surveillance Court to modify or set it aside. In recognition that the Government's response may include classified information, the bill provides that the court shall first review the Government's submission ex parte and in camera. Of course, those parts of the Government's submission that are neither classified nor otherwise law enforcement sensitive should then be provided to the applicant without restriction. The bill also provides that protected information, if necessary to make an accurate determination about the reasonableness or oppressiveness of the order, could be provided to the applicant under appropriate security procedures and protective orders.

By a margin of one vote, the Committee rejected an amendment (also set forth in the appendix to these views) that would have conformed Title V to a key aspect of other major titles of the Foreign Intelligence Surveillance Act. Every other title establishing a method of obtaining foreign intelligence information—Title I on electronic surveillance, Title III on physical searches, and Title IV on pen registers and traps and traces—provides for exercise of emergency power by the Attorney General. These provisions permit the Attorney General to act when an emergency requires immediate action.

The amendment, offered by Vice Chairman Rockefeller, adhered closely to the emergency provisions in FISA's other titles. If an emergency requires production before a FISA Court order can be

obtained, the amendment would authorize the Attorney General to issue an order for production that has the same effect as an order issued by the FISA Court. The safety check on the Attorney General's power is that at the time of issuing that order the Attorney General would be required to notify the FISA Court (as the Attorney General must do for emergency use of other FISA powers) and then apply "as soon as practicable" for a judicial order requiring production. If the application is granted, the Attorney General may continue to use the information obtained under his emergency order. If the application is denied, then the information obtained under the order may not be used.

In sum, under the Rockefeller amendment the Attorney General would be able to act rapidly in an emergency as long as the court is notified and a process, leading to an authoritative ruling of the court, is begun as soon as practicable. In that way, FISA would protect—as it does for electronic surveillance, physical searches, and pen registers—the ability of the Attorney General to act with dispatch while ensuring prompt judicial review. The amendment merits adoption in the course of the Senate's consideration of this bill.

One argument offered in Committee against adding emergency authority to Title V of FISA is that this authority is unnecessary in light of the administrative subpoena power that the bill would grant to the Attorney General. Whether Congress will create a new administrative subpoena authority is, at the present time, only speculative. Title V of FISA is not speculative. It exists. It can and should be improved.

But even if Congress does establish a new administrative subpoena authority, the Department of Justice may conclude, in particular cases, that it advances the Government's interest in the efficient investigation of national security matters to proceed under Title V, including by means of emergency record production orders. For example, emergency orders under Title V may relate closely to other orders in an investigation, such as for electronic surveillance or pen registers. Under the administrative subpoena section of the Committee's bill, legal challenges to those subpoenas may occur in district courts around the country rather than in the Foreign Intelligence Surveillance Court, depending on who goes to court first. By proceeding under Title V, the Government can ensure that all matters about a particular investigation are handled by one court. The Rockefeller amendment would enable the Government to have both an emergency record authority and the ability to consolidate judicial proceedings in one court.

3. Change in Definition of "Foreign Intelligence Information"

Section 202 of the bill amends the definition of "foreign intelligence information" in Title I of the Foreign Intelligence Surveillance Act (FISA). As the definition in Title I of "foreign intelligence information" is also the definition used in other titles of FISA—on physical searches, pen registers and traps and traces, and orders for the production of business records and other tangible things—the amendment to the definition will have an impact on all the investigative methods authorized by FISA.

Section 202 alters the definition of "foreign intelligence information" by providing that the term includes "protection [of the United States] by use of law enforcement methods such as criminal prosecution." Law enforcement methods such as criminal prosecution are key methods of protecting the United States. The question, however, is whether this change in definition would muddy or even jeopardize a salient achievement of the PATRIOT Act, namely, the "significant purpose" test in Section 218.

Section 218 eliminated the prior test, known as the "primary purpose" test, that had been applied by courts and the Department of Justice before the PATRIOT Act. That test had required that the "primary purpose" of FISA collection had to be obtaining foreign intelligence information rather than evidence of a crime. As described by the Department of Justice in a report to the Committee on April 1, 2005, Section 218 eliminated the primary purpose test by allowing FISA electronic surveillance or physical searches to be authorized if foreign-intelligence gathering is a "significant" purpose, thereby eliminating the need for the courts to compare the relative weight of the "foreign intelligence" or "law enforcement" purpose of the search.

But while a foreign intelligence purpose need not be dominant, the "significant purpose" test requires that there be at least "some" such purpose. The Foreign Intelligence Surveillance Court of Review recognized this when it declared: "Of course, if the court concluded that the government's sole objective was merely to gain evidence of past criminal conduct—even foreign intelligence crimes—to punish the agent rather than halt ongoing espionage or terrorist activity, the application should be denied." In re: *Sealed Case*, 310 F.3d 717, 735 (U.S. FISCR 2002).

The provision of the bill, which was retained at markup by only one vote, would negate that holding of the Foreign Intelligence Surveillance Court of Review and gut the "significant purpose" test in Section 218 by allowing the use of foreign intelligence powers when the sole purpose is to gain evidence of past crimes. By doing so, this provision of the Committee bill could invite a challenge to the constitutionality of FISA based on the argument that if the sole purpose of a FISA order is to obtain evidence of a past crime then the courts must decide whether FISA satisfies the warrant clause of the Fourth Amendment.

The Administration has not requested that Congress change the definition of "foreign intelligence information." Neither the Attorney General nor the FBI Director, in their appearance before the Committee, suggested a desire to change the definition of foreign intelligence information. There has been no showing, in any open or closed setting, that the present and longstanding definition of foreign intelligence information has impeded a single foreign intelligence investigation or criminal prosecution. Nor did the FBI inform Senator Feinstein, in her discussions with the Bureau about her amendment, that it opposed her amendment to strike the provision.

A former Department of Justice official whose service included the current Bush Administration and who was called by the Committee in anticipation that he would address this matter, cautioned:

> First, Section 203 of the Committee's bill would further expand governmental power at a time when the Department of Justice itself has not asked for broader authority. Second, a related point, I fear that any operational benefit from the amendment would not justify the resulting cost in uncertainty about the state of the law. (Testimony of David S. Kris, former Deputy Associate Attorney General, May 24, 2005.)

The Section 203 referred to in Mr. Kris's testimony is Section 202 of the bill as reported.

Not only has the change in the definition of foreign intelligence information not been requested by the Administration, but the Administration has not brought to the Congress's attention any problem with information sharing created by either the PATRIOT Act or the Foreign Intelligence Court of Review decision. To the contrary, as is well known, the Attorney General and the FBI Director credit the PATRIOT Act and the Foreign Intelligence Surveillance Court of Review decision with helping to bring down the "walls" that blocked coordination and cooperation among intelligence and law enforcement officials in the past.

At best, Section 202 of the bill is intended to correct a hypothetical problem. Moreover, the hypothetical is unlikely to arise. It would require a situation in which the Government had sufficient information to demonstrate probable cause that an individual is an agent of a foreign power but has no present interest in the foreign intelligence information that would be collected by a FISA surveillance or physical search of that individual.

Thus, Section 202, which will bring uncertainty to a critical area of the law, addresses neither a realistic nor a demonstrated need. It should be deleted.

4. Roving Wiretaps

Senator Levin offered an amendment that would have required roving electronic surveillance orders under FISA to include a description of the target of the surveillance "sufficiently specific to give some confidence" that the person surveilled is actually the same target for whom the court found probable cause to believe is an agent of a foreign power. The amendment sought only to establish in law what we understand to be current Justice Department practice. Adoption of the amendment would have helped improve public confidence that the government will not be listening in on the private conversations of innocent Americans using roving FISA wiretap orders. Unfortunately that amendment was defeated, by a margin of one vote.

Roving wiretaps permit electronic surveillance of people who may be taking steps, such as switching cell phones or using multiple pay phones or computer terminals, to evade electronic surveillance at a particular location. Under criminal law, an application for a roving wiretap must identify the person against whom the wiretap is sought and make a showing that there is probable cause to believe that the actions of that person could have the effect of thwarting interception from a specific facility. Under criminal law, a judge may issue a roving electronic surveillance order if he or she deter-

mines that such a showing has been adequately made. Under FISA, the FISA Court judge must issue an order if he or she finds probable cause, based on the application, that, in addition to other requirements, the target of the electronic surveillance is a foreign power or an agent of a foreign power. The judge's order authorizing the surveillance must specify the identity of the target only if that identity is known. If it is not known, the order need only contain a description of the target.

In an unclassified portion of a May 24, 2005 letter from the Department of Justice to the Chairman, the Department stated that under FISA:

> 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 an agent of a foreign power. As a result, section 206 is always connected to a particular target of surveillance. (Emphasis added.)

Requiring in law, as the Levin amendment sought to do, that FISA electronic surveillance orders be sufficiently specific would be entirely consistent with the Department's statement.

5. MAIL COVER

In the 1970's, both a presidential commission (chaired by Vice President Nelson Rockefeller) and a Senate select committee (chaired by Senator Frank Church) brought to light significant abuses by government agencies concerning intrusive examination of the mail. To meet the twin goals of ending abuses while providing federal and state investigators with access to information that can be gleaned from examining envelopes, but not reading the content of sealed letters without appropriate judicial warrants, the Postal Service promulgated regulations. These regulations have been in place for thirty years.

While the Committee has not held a hearing on mail cover issues, its report identifies a few shortcomings with the regulations. In response, the Committee's bill proposes an entire new title of FISA to govern the examination of mail covers. It is not at all clear why legislation is needed. The several issues identified in the Committee report concerning the regulations can be addressed expeditiously by two agencies of the federal government—the Department of Justice and the Postal Service—working together cooperatively to amend the regulations or improve practices to the extent required. It is our hope that those efforts will begin promptly. If successful, they may obviate the need for legislation.

For some of us, problems in the Committee bill, several of which would have been remedied by the amendments described above, were sufficient to warrant a "no" vote on the bill. For others of us, a "yes" vote was warranted by the importance of proceeding further in the legislative process with a bill that includes the renewal of PATRIOT Act authorities and modifications that correct some of

the present defects in the law. All of us are united in the conviction that improvements in the bill are essential before final passage. Adoption of the amendments described above would be an important step toward achieving a bill that provides a long-term basis for effective national security investigation authority within the boundaries of our Constitution and values.

JOHN D. ROCKEFELLER IV.
CARL LEVIN.
DIANNE FEINSTEIN.
RON WYDEN.
EVAN BAYH.
BARBARA A. MIKULSKI.
JON S. CORZINE.

APPENDIX—TEXT OF AMENDMENTS

ADDITIONAL AND MINORITY VIEWS OF SENATORS ROCKEFELLER, LEVIN, FEINSTEIN, WYDEN, BAYH, MIKULSKI, AND CORZINE

1. AMENDMENT PROPOSED BY SENATOR FEINSTEIN ON EMERGENCY USE OF ADMINISTRATIVE SUBPOENAS

[To be inserted in Committee bill, as reported, as a new Section 802(d)]

(d) REQUIREMENT FOR EMERGENCY USE.—A subpoena may be issued under this title only after the Attorney General, or a designee of the Attorney General, or the Director of the Federal Bureau of Investigation, or a designee of the Director in accordance with subsection (a), certifies, whether in writing or orally (and if certified orally, then reduced to writing as soon thereafter as possible), that—

(1) it is impracticable to obtain in a timely fashion the records or materials to be required to be produced by such subpoena pursuant to a subpoena or order issued by the Foreign Intelligence Surveillance Court under other provisions of this Act or pursuant to other means; and

(2) there is a reasonable belief that there is an emergency need for such records or materials in order to protect United States persons against terrorism.

(b) REVIEW AND APPROVAL.—A subpoena may be issued under this title only after the review and approval, whether orally or in writing, of the subpoena by any of the following:

(1) The Attorney General.

(2) The Deputy Attorney General.

(3) The Associate Attorney General.

(4) An Assistant Attorney General, including an acting Assistant Attorney General.

(5) A United States Attorney.

2. AMENDMENT PROPOSED BY VICE CHAIRMAN ROCKEFELLER ON EMERGENCY FISA RECORD AUTHORITY

[To be inserted in the Committee bill, as a new Section 211(b), with present subsections (b)–(e) renumbered accordingly]

(b) EMERGENCY ACCESS.—

(1) Notwithstanding any other provision of this section, when the Attorney General reasonably determines that—

(A) an emergency situation exists with respect to the production of tangible things for an investigation described in subsection (a) before an order authorizing production of

such tangible things can with due diligence be obtained; and

(B) the factual basis for the issuance of an order under this section to approve production of such tangible things exists,

the Attorney General may issue an order requiring production of such tangible things, which order shall have the same effect as an order issued by the court established by section 103(a), if a judge having jurisdiction under section 103 is informed by the Attorney General, or a designee of the Attorney, at the time of the issuance of such order that the decision has been made to require production of such tangible things under this subsection and an application in accordance with this section is made to that judge as soon as practicable thereafter.

(2) In the event that an application under paragraph (1) is denied, or in any other case where no order is issued by the court established by section 103(a) approving access to tangible things, no information obtained or evidence derived from the production of tangible things under paragraph (1) shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from the production of tangible things under paragraph (1) shall subsequently be used or disclosed in any other manner by any officer or employee of the Federal Government without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(3) The denial of an application under paragraph (1) may be reviewed as provided in section 103.

3. AMENDMENT PROPOSED BY SENATOR LEVIN ON ADMINISTRATIVE SUBPOENA NONDISCLOSURE REQUIREMENTS

[To be inserted in the Committee bill, as reported, as new paragraphs (3) and (4) of Section 802(b)]

(3) LIMITATION ON DURATION OF NONDISCLOSURE REQUIREMENTS.—Except as provided in paragraph (4), the prohibition on disclosure under subsection (a) with respect to a subpoena under section 802 shall expire 90 days after the date of the issuance of the subpoena.

(b) EXTENSION.—The Foreign Intelligence Surveillance Court, or the United States district court in which a person or entity subject to a prohibition on disclosure under subsection (a) resides or does business, may, upon application by a person authorized to issue a subpoena under section 802, extend a prohibition on disclosure under subsection (a) with respect to a subpoena issued under section 802 for one or more additional periods of not more than 90 days upon a showing by the applicant that a danger to the national security of the United States may result from disclosure that such subpoena was received or records were provided pursuant to this

title. Each extension for a period under this paragraph shall require a new application under this paragraph.

ADDITIONAL VIEWS OF SENATOR MIKULSKI

INTRODUCTION

Following the tragedy of September 11th, it was critical to provide law enforcement in the United States with the tools it needed to effectively fight the war on terror. Our intelligence, counterterrorism and counterintelligence experts needed new authorities to protect our country, our people and our treasured allies.

It is our goal to stop terrorists in their tracks and to keep our citizens safe. But we must do so while providing appropriate checks and balances which protect the fundamental constitutional rights on which this nation was founded.

We struck that balance in the PATRIOT Act by providing law enforcement with greatly expanded powers while also creating sunsets for the most controversial powers. We realized the potential for abuse in creating these broad new provisions and it was our constitutional responsibility to make sure that these new authorities were not abused or misused. That's why sunset provisions are so important.

This reauthorization is using the opportunity of the sunsets to review how the PATRIOT Act has been used and how it can be improved. There are features of the bill being reported out by the Intelligence Committee that I agree with. However, I have several serious concerns about some of the provisions, including most importantly the failure to include sunsets which would allow us to conduct future periodic reviews. We must have sunsets and we must review how these new powers are being used or misused.

I'm also concerned with the dramatic expansion of power to conduct intelligence gathering solely for criminal prosecutions. The administration did not even ask for such sweeping new authority. The bill also grants administrative subpoena power without appropriate limitations. These provisions greatly expand current authorities and how intelligence investigations are conducted. I believe that changes to this bill are necessary and that any unlimited extension of controversial provisions should be fully debated in the sunshine and decided by the full Senate.

SUNSETS ARE ESSENTIAL

This bill makes permanent the original provisions that were set to sunset at the end of this year. Law enforcement agencies say that these tools are needed to gather intelligence to fight the war on terror. I take very seriously the needs of law enforcement and the need to fight terrorism. But, I am concerned that some of these provisions are too broad and that we need to add appropriate checks on the powers. We need to know the specifics about how and when they are being used and whether they are impacting the constitutional rights of Americans.

I believe that we do not need to make these provisions permanent—extending the sunsets of these provisions for another four years does no harm. It provides law enforcement with the ability to use all the same tools that they now have under the PATRIOT Act. At the same time, it provides for oversight and requires the Congress to periodically review how the powers are being used. We need to know how often they are being used, in what context, and who is impacted.

Extending the sunsets for four more years allows this expansion of power to be checked to ensure that it is not undermining fundamental constitutional protections.

KEEP THE SIGNIFICANT PURPOSE TEST FOR INVESTIGATIONS

The PATRIOT Act provided law enforcement with broad authority to conduct surveillance and searches where collecting foreign intelligence was the "significant purpose" of the investigation. This broad authority has worked well.

Both Attorney General Gonzales and FBI Director Mueller have praised the "significant purpose" standard and the administration has not requested any change to the standard. Yet, this bill would change the PATRIOT Act to allow the collection of intelligence solely for the use as evidence in a criminal prosecution.

This unrequested change is unnecessary and unwise. Indeed, Senator Feinstein has indicated that the FBI did not object to her amendment to strike this provision, which I supported. This change will create uncertainty between the criminal law and intelligence gathering fields where guideposts are already well established and working well.

ADMINISTRATIVE SUBPOENAS SHOULD BE FOR EMERGENCIES

The Administration has argued that it needs the authority to issue administrative subpoenas because of emergency situations. But, this legislation adds far-reaching administrative subpoena powers that are not limited. There is no need for such broad authority and the potential for abuse of constitutional rights is too great. I cannot support such unrequested and unlimited power.

I understand that we need to make sure there are no obstacles when immediate action is needed to prevent a terrorist attack or the loss of life. Therefore, if the power to issue administrative subpoenas is included in this bill, it must be limited to exigent or emergency circumstances only.

CONCLUSION

I believe that the Senate has a lot of work to do as this bill moves forward. This bill adds some provisions for checks and balances and judicial review—but more are needed. Law enforcement must have the tools they need to fight the war on terror. But, we must also protect the role of our federal courts to make sure that there is no abuse of power.

We need to strike the appropriate balance—protecting national security while protecting constitutional rights.

BARBARA A. MIKULSKI.

ADDITIONAL AND MINORITY VIEWS OF SENATORS CORZINE, LEVIN, WYDEN, AND MIKULSKI

The current legislation, by permanently repealing the sunset on Section 215 of the USA PATRIOT Act, unnecessarily preempts a critical review of and debate on the impact of this controversial and far-reaching provision. We believe that the sunset should be extended for another four years, through December 31, 2009.

Simply repealing the sunsets included in the USA PATRIOT Act deprives Congress and the American people the opportunity to fully explore the implications of the law. The sunset on Section 215, which provides broad authority to seek business records, including from libraries, booksellers and medical practitioners, through FISA, is particularly important. Of all the new authorities provided in the USA PATRIOT Act, Section 215 has generated the most public concern. The FISA court operates in secrecy and the targets of Section 215 warrants are unlikely to ever learn that their records have been sought. The sensitivity of the information subject to a Section 215 warrant and the lack of public information about how the provision has been used have prompted calls for a public debate about how both to combat terrorism and protect civil liberties.

On April 5, 2005, in apparent response to these concerns, the Attorney General publicly announced that Section 215 had been used 35 times, and never for libraries or booksellers, or to obtain medical or gun records. While we welcome this disclosure, we note that this one-time, discretionary declassification came only as Congress was considering the reauthorization of Section 215. An extension of the sunset will encourage further disclosures, which serve to reassure the American public that one of the most controversial and far-reaching provisions of the USA PATRIOT Act have not been abused.

Over the next four years, Congress will be reviewing critical information related to the use of Section 215. New reporting requirements in the current legislation cover the use of Section 215 to obtain records on the sale, rental or delivery of books and other reading material, firearms, health information, and tax returns. The legislation also requires a report on "discreet inquiries," a method through which the FBI has sought certain business records, including from libraries, without a FISA warrant. While we do not discourage informal information-gathering efforts, the frequency with which such inquiries are made, the kind of information sought, and the targets involved are relevant to whether Congress should permanently enact Section 215.

While the information released by the Attorney General on April 5 suggests a judicious use of Section 215 to date, it does not provide any check on how this power will be employed in the future. The Intelligence Community is currently in flux, with the recent confirmation of the Director and Deputy Director of National Intel-

ligence and the creation of the National Counterterrorism Center (NCTC). The FBI faces a myriad of challenges as it redirects its resources toward preventing terrorism, from information technology to a much-needed cultural shift within the Bureau. Under these circumstances, it is far too early to project how the broad authorities conferred by the USA PATRIOT Act may be used in the future.

Perhaps most importantly, the very institution mandated by Congress to oversee these new authorities has yet to be established. The Privacy and Civil Liberties Board, established in the Intelligence Reform and Terrorism Prevention Act of 2004, is responsible for overseeing the implementation of laws related to protecting the nation against terrorism. Before Section 215 becomes a permanent authority, without the Congressional and public scrutiny that comes with a sunset, it is critical that the Board be in place to monitor its use.

Finally, we note that the current legislation modifies Section 215. These modifications, which include a "relevance" standard and new provisions related to disclosure, represent an ongoing Congressional debate about the extent and limits of the authorities provided by Section 215. If they are passed into law, it will be critical that Congress review how they are used, how they effect the overall implementation of Section 215, and whether further modifications are necessary. In this context, the permanent repeal of the sunset is unwarranted.

Congress as well as the American people should continue the public dialogue over the expansive powers given to the FBI under the USA PATRIOT Act and how to combat terrorism while protecting the basic rights of all Americans. By seeking to extend the sunset on Section 215, we encourage that dialogue.

JON S. CORZINE.
CARL LEVIN.
RON WYDEN.
BARBARA A. MIKULSKI.

MINORITY VIEWS OF SENATOR FEINSTEIN

Although I support the reauthorization of the sunsetting provisions of the PATRIOT Act, I cannot support the legislation in its present form. This legislation contains two provisions that vastly expand current authorities and greatly expand the power of the Federal Bureau of Investigation in conducting intelligence investigations and prosecuting criminal activity. It is disappointing that the majority has refused to accept amendments to place reasonable limits on these new authorities.

Section 202 of the Committee's legislation presents a fundamental change to the laws governing investigations conducted under the Foreign Intelligence Surveillance Act (FISA). The addition of criminal prosecutions to the definition of "foreign intelligence information" allows, for the first time ever, the FBI to use FISA to collect intelligence solely for the use as evidence in a criminal prosecution. This change would undermine current law, passed as part of the PATRIOT Act in 2001 that requires the FBI to articulate a significant intelligence purpose in conducting any FISA investigation. This standard has been praised by Attorneys General Ashcroft and Gonzales and by FBI Director Mueller as a key component to their ability to fight the war on terror.

There has been no request by the Administration for this change to the law, and the FBI did not object to my amendment to strike this language. Section 202 of this legislation undermines the significant purpose test, removes the distinction between intelligence and law enforcement operations within the FBI, and threatens to create uncertainty in the currently well established relationship between intelligence and criminal proceedings.

Section 213 of this legislation authorizes the FBI to issue administrative subpoenas to compel information on anything that can be claimed relevant to an ongoing investigation. This authority can be delegated to an FBI field office without check of a Department of Justice attorney or prior court approval, as is currently required for FISA Business Records requests. As approved by the Committee, this provision would amount to a fishing license of unprecedented proportions.

My amendment to Section 213 would have made two modest but critical changes to this provision: it would have limited the use of administrative subpoenas to emergency situations where life was on the line—which was the only case where the Administration has claimed a need for this authority; and the need for approval (even if done over the phone) by a U.S. Attorney or Department of Justice official.

Proponents of the intelligence administrative subpoena point out that there are already 335 different cases where the federal government has subpoena authority. Very few of these cases involve the Department of Justice, and none pertain to intelligence. More im-

portantly, in those cases, a crime has taken place and a subpoena has to hold up to scrutiny in court. In the intelligence regime, a record just has to relate to something that might happen in the future. There will almost never be any court review, and when there is, the government can argue its case in secret. In fact, the party being issued with the subpoena will almost never be able to disclose the very existence of the subpoena. In these cases, when the government is exercising its authorities behind closed doors, we should be requiring extra safeguards to protect civil liberties, not fewer.

Finally, I supported and regret the defeat of Vice Chairman Rockefeller's amendment to provide the Attorney General with emergency powers under FISA to demand access to business records. This would not have replaced the administrative subpoena authority in the legislation, and would simply have provided emergency use authority as is already on the books for electronic surveillance and physical searches under FISA.

It appears that if administrative subpoena authority is enacted, the FBI will find it an easier mechanism for obtaining records than the FISA Business Records authority provided under the PATRIOT Act. It is thus irrelevant that the Committee has included good legislation to improve these FISA statutes as the authority will not be used. I find it alarming that the Committee has chosen to replace, in effect, the most controversial element of the PATRIOT Act with a far broader subpoena authority subject to fewer checks on abuse.

In short, the Committee's legislation strays from the well-crafted and working balance struck in the PATRIOT Act. The provisions in Sections 202 and 213, neither of which had strong Administration support or justification, make fundamental changes to the way intelligence investigations are authorized and conducted. Both raise serious questions that need to be answered before this legislation is passed by the Senate.

DIANNE FEINSTEIN.

MINORITY VIEWS OF SENATORS WYDEN AND CORZINE

There are a number of provisions in this legislation that give cause for concern. Perhaps the most troubling, however, is section 213, which gives the FBI unprecedented, excessively broad authority to write its own administrative subpoenas.

We are opposed to giving the FBI authority to write administrative subpoenas for foreign intelligence investigations. The Bureau failed to make the case for such new power and giving the FBI the authority to demand just about anything from anybody, with no independent check, simply by claiming that it is "relevant" to a national security investigation would lead us down a very dangerous path. Citizens have a right to feel secure that their government is not spying on them or soliciting information secretly without, at a minimum, authorization from a grand jury, federal judge, or the Foreign Intelligence Surveillance Court.

The FBI already has access to the waterfront of personal information through the Foreign Intelligence Surveillance Act, or FISA warrant process. All it has to do is go before a judge and explain why the information is relevant. By giving the FBI the authority to write its own administrative subpoenas, we would be removing even this last, modest safeguard.

Administrative subpoenas are currently used by many federal agencies in many different contexts—from investigating labor and environmental violations to criminal investigations. However, administrative subpoenas are extremely limited in application and use. Congress has explicitly limited the authority of the FBI to issue administrative subpoenas and set specific limits on what type of information the FBI could obtain and from whom. And the FBI is held firmly accountable, under all of the administrative subpoena powers presently held by the Bureau, to grand juries and federal courts of law, which ultimately review the issuance of such subpoenas.

Except in a few very limited cases, administrative subpoenas are not used for national security investigations. That is because national security investigations are different from criminal investigations. They are conducted in secret, and do not require evidence of a crime. This is why there are different rules for the two types of investigations. Ignoring the distinction between the two is both inappropriate and unwise.

As proposed, these subpoenas would be incredibly broad in scope. They could be used to gain access to citizens' credit records, video rentals, medical records, gun purchases—effectively, they could be used to obtain just about anything. And they would be used to obtain this information without the knowledge, perhaps ever, of the individuals whose records are seized.

These subpoenas would only be seen by a judge if the recipient of the subpoena decided to challenge it. Even if the recipient was

properly notified of his or her right to challenge, they might not have the time or resources to do so.

For example, there are 56 FBI Field Offices—one in almost every major American city. The head of the local field office could issue an administrative subpoena to a hospital director and ask for all the hospital's medical records, simply by claiming that the records were relevant to an investigation. It will be difficult, if not impossible, for a third party such as a hospital to know whether the subpoena was issued reasonably. And it is extremely unlikely that third party record holders would challenge the issuance of national security administrative subpoenas. Consequently, patients would not even know their records had been seized. They would be totally in the dark.

Even the FBI acknowledges that it can get all the information it could possibly need with the investigative powers it currently has. The only reason the FBI has suggested for supporting administrative subpoenas is speed. It says that the FISA warrant process is sometimes too slow for time-sensitive emergency situations.

There were several amendments filed by the minority side that would have addressed the FBI's concern for speed without jeopardizing the privacy of law-abiding Americans. The simplest way to do this would be to modify the FISA statute to provide for emergency circumstances.

Creating an emergency provision under FISA would give the FBI adequate authority to respond to emergency situations, which the FBI concedes would be very rare, without giving the Bureau unnecessarily broad powers that could be used for fishing expeditions, or without any showing of law-enforcement need.

The emergency provision would give the Attorney General the authority to declare that particular business records are needed immediately to respond to an emergency situation. Under these circumstances, the FBI could notify a judge that it is serving an emergency warrant, and then make a more detailed application after responding to the emergency. For example, if the FBI learned that a group of terrorists was preparing for an attack and had rented a car at a particular location, the Attorney General could declare that this was a time-sensitive emergency. Then the FBI could notify a judge that it is serving an emergency warrant on the rental car agency, and demand that the agency give the Bureau descriptions and license numbers of all the cars the terrorists rented that morning. After the FBI had responded to the emergency, it would have to go back to the judge and formally apply for the warrant. If there was a case where the judge decided that the FBI had acted inappropriately, and refused to grant the warrant, then the agents would be prohibited from using or divulging the information that they had taken.

It is essential for the FBI to have this sort of emergency power; however, it is equally essential that we provide automatic review by a judge to safeguard against abuse. We must never forget our ultimate goal: to make the United States safer while protecting the rights of all Americans. It cannot be an either/or question. We must expand the powers of the FBI to combat terrorism while ensuring that real safeguards exist to preserve our civil liberties.

This is why administrative subpoena authority should be struck entirely from this legislation.

We encourage our colleagues outside the committee to consider this legislation very carefully, and we look forward to continuing this debate on the Senate floor.

RON WYDEN.
JON S. CORZINE.

○