U.S. Department of Justice

Office of Information Policy

Telephone: (202) 514-3642

Washington, D.C. 20530

SEP 9 2009

Ms. Marcia Hofmann
Staff Attorney
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110-1914

Re: OLA/09-R0241
CLM:TEH:JK

Dear Ms. Hofmann:

While processing your Freedom of Information Act request dated September 22, 2006, in which you requested specific records pertaining to the pen register statute, 18 U.S.C. §§ 3121-3127, the Criminal Division located two documents, totaling fourteen pages, which it referred to this Office for processing and direct response to you. This response is made on behalf of the Office of Legislative Affairs.

I have determined that these documents are appropriate for release without excision and copies are enclosed.

Inasmuch as this constitutes a full grant of the documents that were referred by the Criminal Division, for processing on behalf of the Office of Legislative Affairs, I am closing your file in this Office.

Sincerely,

Carmen L. Mallon
Chief of Staff

Enclosures

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

November 29, 2001

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

Dear Mr. Chairman:

Please find enclosed answers to questions to the Attorney General in your letter dated November 1, 2001. The Department appreciates your legitimate oversight interest in implementation of the USA-PATRIOT Act of 2001.

The Attorney General looks forward to testifying before the Committee on December 6, 2001. Please do not hesitate to contact me if we can be of any assistance on this or any other matter of mutual concern.

Sincerely,

Daniel J. Bryant
Assistant Attorney General

Enclosure

cc: Senator Orrin G. Hatch
Ranking Member

Attorney General's Responses to Questions Submitted by Senate Judiciary Committee Chairman Patrick Leahy on November 1, 2001

September 25, 2001 Judiciary Committee Hearing

1. **Question 15 cited press reports that the Chief Judge of the FISA Court wrote to you raising questions about FISA wiretap requests. I asked for communications between the FISA Court Judges and the Department of Justice on such matters, as well as for Justice Department and FBI reviews of FISA surveillance authorizations. I am disappointed that the Department has not promptly replied and is still considering the Committee's request. Please provide (a) a full and complete description of the factors under consideration in determining whether to respond to the request; and (b) information on how long it will take for the Department to "consider the Committee's request for documents."**

Answer: The Office of Intelligence Policy and Review (OIPR) provided the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence with a description of this incident in its semi-annual report submitted pursuant to statutory authority in April 2001. The Office of Professional Responsibility is currently investigating the occurrence of alleged factual errors in and omissions from two different sets of FISA applications. The investigation is being conducted jointly by the Justice Department's Office of Professional Responsibility and the FBI's Office of Professional Responsibility because the applications at issue were prepared jointly by the FBI and OIPR.

In regard to your request for copies of correspondence between the FISA Court and the Department, as your staff was informed orally in followup to the Department's response to original Question 15, the Department believed it necessary to review considerations related to the appropriateness of providing Congress with access to correspondence that originated with the FISA Court or were created in response to such correspondence. The Department has completed that review and determined that it may provide that access. Accordingly, Department staff will work with Committee staff to make this correspondence available to them for their review. Because the investigation being conducted jointly by the Department's and the FBI's Offices of Professional Responsibility is active and ongoing, access to documents that involve reviews of this matter would not be appropriate at this time.

2. **Question 19 requested a description of administrative and regulatory changes made since you took office in the effort against terrorism. The response cites several memoranda and "an initiative of the Department, working with its client agencies, to make FISA more efficient and more effective against foreign terrorist and other intelligence targets in the United States." Please provide (a) a full and complete**

description of the FISA reform process, which you say "continues"; and (b) a full and complete description of any reorganization plan for the FBI that you are contemplating as part of your effort to make FISA more efficient and effective.

Answer: In January 2001, the Office of Intelligence Policy and Review (OIPR) began to meet informally with its client agencies to solicit reforms to the provisions of, and practice under, FISA and practice under Section 2.5 of Executive Order 12333 in order to make both more efficient and more effective. In March 2001, OIPR hosted the first of several interagency meetings to consider several proposed reforms to FISA. Out of that process came two reforms to FISA – extending renewal periods and enabling roving surveillance – that the Attorney General approved in August 2001 for interagency clearance for submission to Congress. These two reforms are reflected, with modifications, in sections 206 and 207 of the USA-PATRIOT Act of 2001. Out of that interagency process, at least indirectly, have also come additional proposals – to extend deadlines for emergency approvals, to include individual terrorists in the definition of "foreign power," and to broaden the definition of "foreign power" to include priority intelligence targets identified in Presidential Decision Directive 35 – that have been submitted for interagency clearance for submission to Congress. The Department regards this interagency process, which can assess the classified, compartmented, and sometimes conflicting equities of our client agencies, as essential to the effective reform of FISA and is committed to its continuation.

3. **In response to question 52 you state that "The restrictions on the sharing of grand jury and other information would...apply to subsequent transfers and use of that information." What will be done to ensure that non-law enforcement personnel to whom the grand jury, wiretap and other criminal justice information is transferred recognize and protect grand jury information?**

Answer: Section 203 of the USA-PATRIOT Act authorizes any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official receiving grand jury or wiretap information pursuant to the Act to use that information "only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information." The Department is in the process of consulting with the intelligence community to establish appropriate procedures for the handling of shared grand jury and wirtetap information. Although the details are still being developed, it is anticipated that the procedures will require that shared grand jury and Title III wiretap information be appropriately marked and secured by the recipient, and that whenever possible subsequent sharing of the information by the recipient will be made in a manner that does not reveal "matters occurring before a grand jury" or violate the disclosure prohibitions of 18 U.S.C. 2517. With respect to shared grand jury information, an attorney for the government is required by Section 203(a)(1) of the Act to file a notice with the Court identifying the agencies or entities to which the disclosure was made. Accordingly, to the extent that the initial recipient believes it is

necessary to share unredacted grand jury information with another department, agency, or entity, the procedures will require appropriate consultation and notice to an appropriate federal prosecutor so that the statutorily required notice can be filed with the Court.

4. **Question 75 asked how we can be sure that the new authority to obtain education records will not be used to harass students who are merely exercising their First Amendment rights of political expression. Your response states that Justice Department policy and FBI practice "ensure that no such harassment will occur, by requiring that investigations be predicated on facts: before initiating an investigation (i.e., beyond the measured, limited and preliminary checking out of allegations and leads), the FBI must have facts and circumstances reasonably indicating that a federal crime has been, is being, or will be committed." Please explain how this response applies to Justice Department policy and FBI practice under the Attorney General's Guidelines for FBI Foreign Counterintelligence Investigations and FBI Domestic Security Investigations, which may allow FBI investigations of United States persons without a conventional criminal predicate.**

Answer: FBI practice in Domestic Security investigations is governed by Department of Justice policy set out in the "Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations," issued by then-Attorney General Thornburgh in 1989 (the "Criminal/DST Guidelines"). The Criminal/DST Guidelines provide guidance for all investigations by the FBI of crimes and crime-related activities, and in particular, the standards set out in those guidelines govern the circumstances under which an investigation may be begun. The Criminal/DST Guidelines provide that no investigation may be initiated unless there are "facts or circumstances [which] reasonably indicate that a federal crime has been, is being, or will be committed." While lower than probable cause, this standard does "require specific facts or circumstances indicating the past, current, or impending violation" of Federal law. A mere hunch is insufficient. The Guidelines also provide standards for the initiation of preliminary inquiries. Preliminary inquiries may only be undertaken where the FBI receives an "allegation or information indicating the possibility of criminal activity." Preliminary inquiries are to be of short duration and confined solely to obtaining the information necessary to make an informed judgment as to whether a full investigation is warranted. It is important to note in this context that the Criminal/DST Guidelines explicitly require that investigations "not be based solely on activities protected by the First Amendment or on the lawful exercise of any other rights secured by the Constitution or laws of the United States."

In addition to General Crimes criminal investigations, the Criminal/DST Guidelines also allow for Domestic Security/Terrorism investigations which are designed to focus on domestic terrorism enterprises. However, the initiation of such an investigation must be based on "facts and circumstances [which] reasonably indicate that two or more persons are engaged in an enterprise for the purpose of furthering political or social goals wholly

or in part through activities that involve force or violence and a violation of the criminal laws of the United States." The standard of "reasonable indication" is the same as that governing the initiation of a general crimes investigation discussed above.

Therefore, Department policy as set forth in the Guidelines and FBI practice in conducting General Criminal or Domestic Security/Terrorism investigations under those Guidelines are designed, among other things, to preclude harassment of students – or other citizens – who are merely exercising their First Amendment rights of political expression.

Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations require that full counterintelligence investigations be based upon specific and articulable facts giving reason to believe that a U.S. person, group, or organization is or may be engaged in certain categories of specific conduct of clear counterintelligence interest. These guidelines specify that any such investigation of a group not focus on unrelated First Amendment activity. Any use of FISA, furthermore, requires that, for any U.S. person, probable cause not be based solely upon activities protected by the First Amendment. 50 U.S.C. 1805(a)(3)(A), 1824(a)(3)(A), 1842(a)(1), 1842(c)(2), 1843(a), 1843(b)(1), Section 501(a)(1) and (a)(2)(B) (replacing 50 U.S.C. 1863).

5. **In response to question 89 about the "content" aspect of Internet routing information, such as a website name or search engine entry, the response states that "an order under the statute could not authorize collection of the subject line of an e-mail, as that clearly contains content. Conversely, the Internet Protocol address ('IP address') or an Internet host name (such as www.cropduster.com) is analogous to the general phone listing for a business. As such, they are plainly not content." Does the Department consider URL codes to be content when used to visit separate locations within an Internet host (such as each separate news and feature article on www.washingtonpost.com)? For example, is www.washingtonpost.com/wp-dyn/articles/A7842-2001Oct17.html comparable to the "subject line" on an e-mail and therefore content?**

Answer: The Department of Justice has been, and will continue to be, sensitive to the legitimate privacy interests of Internet users, and is mindful of the debate over whether "Uniform Resource Locators" (URLs) may constitute content. Indeed, the current practice is not to gather any part of a URL through a pen/trap order. Instead, in appropriate cases, the pen/trap order authorizes collecting "IP addresses" accessed by a criminal suspect, which generally provide no more detailed information than a hostname (e.g., www.washingtonpost.com).

We recognize that reasonable minds may differ as to whether, and at what stage, URL information might be construed as content. As you know, the URL used to access a page

on the Worldwide Web consists of several parts:

(a) A prefix denoting the application protocol to be used, e.g., "http:" for the Hypertext Transfer Protocol used to deliver web pages;
(b) A "hostname" corresponding to the responsible organization (and to the specific web server computer where the website is located), e.g., www.usdoj.gov.; and
(c) A "file path" identifying the location of the requested document, including directory name(s), on the web server's file system, e.g., /criminal/cybercrime/index.html.

Clearly, the prefix and hostname is mere addressing information, and is therefore not content. In fact, a good argument can be made that the entire file path serves simply as the address of a document on the Web and is therefore not content comparable to the "subject line" line of an email message. At the same time, the Department recognizes the concern that, at a certain point along a URL, the information becomes too specific to be appropriately collected by a pen/trap order. Support for that position is found in the House report on H.R. 2975 — a precursor bill to the USA-PATRIOT Act — which expressed the view that a pen register order should not be used to collect "the portion of a URL (Uniform Resource Locator) specifying Web search terms or the name of a requested file or article." H. Rept. 107-236 at 53 (Oct. 11, 2001).

Given the sensitivities of this issue, the field guidance specifically directed agents and prosecutors to consult with Main Justice if there were any questions on whether a specific type of information sought constituted content, noting that "[a]gents and prosecutors with questions about whether a particular type of information constitutes content should contact the Office of Enforcement Operations in the telephone context (202-514-6809) or the Computer Crime and Intellectual Property Section in the computer context (202-514-1026)." In addition, the Department is considering whether specific consultation and/or approval requirements should be instituted in connection with any proposed collection of URL information.

Field Guidance on New Authorities (Redacted), October 26, 2001

6. **On October 26, 2001, your Office of Legislation Affairs provided a copy of Field Guidance on New Authorities (Redacted) Enacted in the 2001 Anti-Terrorism Legislation. On October 30, 2001, you announced to the International Association of Chiefs of Police that a second set of directives would outline a framework of improved information sharing, the information analysis and coordination between federal, state, and local officials. To ensure that the Committee is kept fully informed and to facilitate oversight of the implementation of the USA-PATRIOT Act, please provide (a) a full and complete (unredacted) copy of the Field Guidance; and (b) your assurance that your will provide the Committee on a current basis both redacted and unredacted copies of all such implementing instructions and related directives disseminated to the United States Attorneys, FBI field divisions, and other**

components of the Department of Justice.

Answer:

(a) The Department's Field Guidance on New Authorities in the 2001 Anti-Terrorism Legislation (unredacted version) is an internal document containing sensitive information. However, the Department is willing to make an unredacted copy of the Field Guidance available to the Committee for review.

(b) The Department will continue to notify the Committee when such instructions are issued and make them available as appropriate, in a format consistent with our law enforcement responsibilities.

7. **The reacted Field Guidance does not address several provisions that govern the sharing of foreign intelligence from criminal investigations with intelligence, military, and national security agencies. This information could cover a wide range of political and economic intelligence topics beyond international terrorism. The new law directs the Attorney General to establish procedures for the disclosure of certain information that identifies a United States person, allows the Attorney General to make exceptions in consultation with the Director of Central Intelligence, and requires the Attorney General to develop implementing procedures and a training program for all federal law enforcement agencies. Those procedures should be unclassified to the greatest extend possible. In view of your stated intent to make immediate use of the new authorities, please provide a copy of any procedures that you have developed to implement Sections 203 and 905 and, if no such provisions have been developed, information on the when you plan to complete development of such procedures.**

Answer: Within days of passage of the Act, the Department began the process of developing specific written procedures and guidance to implement Sections 203 and 905, which govern the sharing of foreign intelligence from criminal investigations with other agencies of the Federal Government, particularly the intelligence community. The Department actively is consulting with FBI, CIA, and other interested agencies in this process and will continue to do so. The Department seeks to complete this process as soon as possible while ensuring that the final guidance and procedures are accurate, complete, and comprehensive. As your question reflects, the issue is a complicated one due to the broad scope of what potentially may constitute "foreign intelligence, counterintelligence, and foreign intelligence information" and because of the multiple components within the Justice Department itself as well as the many other Federal Government agencies involved. The Department will keep the Committee informed of the progress of the development of these procedures and will make every effort to issue the final procedures in an unclassified form as is possible.

8. **The Field Guidance on authority for delaying notice of the execution of a warrant provides no guidance on what is a "reasonable period" for delay or what is "reasonable necessity" for seizing items during the search. However, the Department "expects that delayed notice will continue to be an infrequent exception" and that in the weeks ahead "the Department may be providing additional guidance" on this provision. Will you require approval by the Criminal Division before the delayed notice of execution of a search warrant is sought from a court? Will you require approval by the Criminal Division if the period for delayed notice of execution of a search warrant exceed seven days?**

Answer: The Department is considering whether and in what circumstances approval should be required before the delayed notice of execution of a search warrant may be sought. In making a determination in this regard, we will consider what parameters are appropriate for any approval requirement, including the length of delay sought (e.g., seven days), the nature of the investigation involved, and the urgency of obtaining a delayed-notice search warrant in an expedited manner. We will also determine what unit is most appropriate to provide such approval. Finally, we will take into account whether subsequent notice to the Department of Justice would be appropriate in cases where advance approval is not required.

9. **The Field Guidance on the revisions to the pen register and trap and trace laws are incomplete without guidance on the new requirement to use reasonable available technology "so as not to include the contents of any wire or electronic communications." When will the Department issue guidance on using such technology? What technologies have been identified as available for this purpose?**

Answer: Whether or not the specific reference to "contents" in the amendments to section 3121(c) is viewed as merely clarifying pre-existing law, the Department agrees that additional practical guidance on this important subject may be warranted. The Department's Chief Privacy Officer, in consultation with the Office of Legal Policy and the Criminal Division, is reviewing the issue and will draft any appropriate further guidance.

10. **In the provision for intercepting the communications of computer trespassers, the definition of "computer trespassers" includes any person who accesses a protected computer without authorization and explicitly excludes any person who is known to have an existing contractual relationship with the owner or operator. The Field Guidance states, "For example, certain Internet service providers do not allow their customers to send bulk unsolicited e-mails (or 'spam'). Customers who send spam would be in violations of their provider's terms of service, but would not qualify as trespassers–both because they are authorized users and because they have an existing contractual relationship with the provider." The Field Guidance is silent on persons who do not have an existing contractual relationship with the owner or**

operator, but are otherwise permitted by the owner or operator to have such access. Does the Department consider such persons to have authorization? For example, does authorization include the permission given by employers to the employees, libraries to library users, and universities to their students, even if they user violates the owner's policy concerning use of the computer?

Answer: The definition of "computer trespasser" at new 18 U.S.C. 2510(21) makes explicit that new section 2511(2)(i) — providing for monitoring of such trespassers with the consent of the victim — applies only to "a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer." Moreover, section 2510(21)(B) expressly excludes "a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer."

Further, the Department notes that a "contractual relationship" need not be a commercial one, nor even memorialized in a written document. Most employees and university students will have a contractual relationship — even if unwritten — sufficient to make clear that the "computer trespasser" provision cannot be applied to activity known to involve these authorized users.

Moreover, even where such a contractual relationship is arguably lacking, monitoring under section 2511(2)(i) would not be allowed in the case of a person using a system with permission. Thus, a library terminal user permitted to use the library's system would by definition not be "without authorization," and could not be monitored under authority of the new provision, regardless of whether the user commits a violation of the system's terms of use. Similarly, employees or students who are using computer systems with the permission of their employer or university would likewise have "authorization" within the meaning of the statute. The Department's view is that this "contractual relationship" language is really surplusage, since it only states in the affirmative one possible form of authority that a user might possess. Because a trespasser must, by definition, be operating "without authority" (as opposed to "in excess of authority," as those terms are used in 18 U.S.C. 1030) it is not necessary to itemize all the various forms this authority might take.

11. **The Field Guidance regarding Section 809 explains the extension of the statute of limitations relating to certain offenses and state that "the constitutionality of such retroactive applications of changes in statues of limitations is well settled." However, as you know, the Act also changes and expands the substantive nature of certain crimes listed under 18 U.S.C. § 2332b(g)(5)(B) (for instance the expansion of the biological weapons statute, 18 U.S.C. § 175). How does the Department believe that such substantive changes effect the ex post facto analysis? If they do change this analysis, what Field Guidance will the Department issue to ensure that prosecutors do not rely on the incomplete statement contained is the initial**

Guidance in making charging decisions?

Answer: Section 809 of the USA-PATRIOT Act retroactively applies extended limitation periods for certain terrorism offenses. The Supreme Court has recognized that the Ex Post Facto Clause – while prohibiting legislatures from "retroactively alter[ing] the definition of crimes or increas[ing] the punishment for criminal acts," Collins v. Youngblood, 497 U.S. 37, 43 (1990) – does not prohibit "a procedural change [in the law]" . . . "even though it may work to the disadvantage of a defendant." Dobbert v. Florida, 432 U.S. 282, 293 (1977). While the Supreme Court has not yet addressed the issue, the Federal Courts of Appeals "have uniformly held that extending a period of limitations period before the prosecution is barred does not violate the Ex Post Facto Clause." United States v. Grimes, 142 F.3d 1342, 1351 (11th Cir. 1998) (collecting cases). See also, United States v. DeLaMata, 266 F.3d 1275, 1285-1286 (11th Cir. 2001). Thus, Section 809 unquestionably represents a procedural change in the law that does not implicate any substantive interests protected by the Ex Post Facto Clause.

The goal of our field guidance memorandum was, as pertained to Section 809, simply to inform federal prosecutors of the new extended periods of limitation that were enacted and of the constitutional permissibility of applying those extended periods of limitation to criminal offenses that predate the enactment of Section 809. It did not purport to address the question of the retroactive application of any other provision in the Act. We recognize, and believe federal prosecutors across the country recognize, that newly-enacted substantive criminal law provisions cannot be applied on a retroactive basis. We have no reason to believe that federal prosecutors would read our field guidance memorandum – given its clear procedural focus on the permissibility of retroactively applying Section 809's extended periods of limitation – to permit the retroactive application of a newly-enacted substantive criminal law provision, including those that redefine criminal offenses. Accordingly, we do not believe there is a need to provide federal prosecutors with additional guidance on this subject.

12. **The Field Guidance on Section 317, regarding long-arm jurisdiction over foreign money launderers, discusses the new provisions authorizing restraining orders and the appointment of receivers. It then states that this power "appears" to be limited to cases involving long-arm authority over a foreign person. Does the Department intend to seek restraining orders or the appointment of receivers under this new provision in any case where the court is not exercising its long-arm authority over a foreign person? If so, under what circumstances and what would be the Department's good faith basis for believing it could make such a request? If not, what subsequent Field Guidance will the Department issue to clarify its legal position in light of this ambiguous statement?**

Answer: Section 1956(b)(3), as amended by Section 317 of the USA-PATRIOT Act, authorizes the issuance of a restraining order to preserve the availability of assets needed

to satisfy a civil judgment under section 1956(b)(1). (The restraining order provision does not apply to criminal cases or to any type of forfeiture case.) More broadly, section 1956(b)(4) authorizes the appointment of a federal receiver to take custody and control of assets in three circumstances: to satisfy a civil judgment under section 1956(b)(1), to satisfy a forfeiture judgment under section 981 or 982, and to satisfy a criminal fine or restitution order in any prosecution for a violation of section 1956(a) or 1957.

In both subsections (b)(3) and (b)(4), the authority to issue the restraining order or to appoint the federal receiver is assigned to "a court described in [subsection (b)(2)]." Section 1956(b)(2) is the provision that gives a district court long-arm jurisdiction over foreign persons. One possible reading of subsections (b)(3) and (b)(4) is that a court has the power to issue a restraining order or appoint a federal receiver only when it is exercising long-arm jurisdiction over a foreign person, and not when the defendant is a U.S. person. Another colorable reading could be that the reference to "[a] court described in paragraph (2)" means any district court, including but not limited to a court exercising long-arm jurisdiction.

Cases in which the appointment of a receiver pursuant to subsection (b)(4) would be helpful in satisfying forfeiture judgments and preserving assets for the benefit of victims involve foreign defendants only in the rarest circumstances. It would seem inconsistent with the legislative purpose to say that a receiver could be appointed to protect the interests of the United States and the victims of the crime in the fraction of cases that involve foreign defendants and not in the majority of cases that involve domestic defendants. On the other hand, a statement in the legislative history suggests that Congress intended that subsection (b)(3), which contains identical language regarding "a court described in paragraph 2," apply only to those cases involving foreign persons. See 147 Cong. Rec. S11043 (daily ed. October 25, 2001) (statement of Sen. Sarbanes) (stating that a court "dealing with a foreign person" is authorized to issue a pretrial restraining order). It was the Department's intent, in submitting a similar (but textually different) provision to subsection (b)(3), that it apply only to cases involving foreign persons.

As the identical language referring to subsection (b)(2) appears in both subsections (b)(3) and (4), it would be difficult to ascribe one interpretation to the language in one instance and a different interpretation in the other instance. This makes it difficult to state with certainty how the statute should be interpreted. It might be prudent for Congress to enact a clarifying amendment for both subsections (b)(3) and (b)(4). Pending such a clarification, we will not be issuing definitive guidance.

Foreign Intelligence Surveillance Act

13. **The Judiciary Committee intends to conduct meaningful oversight of the Justice Department's use of FISA, especially for law enforcement purposes, and to make appropriate use of the General Accounting Office. Section 108 of FISA states,**

"Nothing in this title shall be deemed to limit the authority and responsibility of the appropriate committees of each House of Congress to obtain such information as they may need to carry out their respective functions and duties." Consistent with this provision, please provide the Judiciary Committee copies of the semiannual reports prepared for the Intelligence Committees and supplement those reports with summaries of all cases in which the primary purpose of the surveillance or search was not to obtain foreign intelligence information.

Answer: The Department of Justice is happy to comply with the requirements of FISA, which appropriately directs the Department to share certain information with Congress so it may fulfill its oversight responsibilities. We have always complied with the reporting requirements of FISA and will continue to do so.

Section 107 of FISA, 50 U.S.C. 1807, directs the Attorney General to submit to "Congress" a report setting forth the total number of applications made and the total number granted, modified, or denied. We submitted our report under section 107 to your Committee, and to its counterpart in the House, last April. See also 50 U.S.C. 1826, 1846, FISA Section 502 (enacted by USA-Patriot Act)

Section 108(a) of FISA, 50 U.S.C. 1808(a), provides that the Attorney General shall on a semi-annual basis "fully inform" the "House Permanent Select Committee on Intelligence and the Senate Select Committee[] on Intelligence" concerning "all electronic surveillance." See also 50 U.S.C. 1826, 1846, FISA Section 502 (enacted by USA-Patriot Act). In contrast, these same provisions require the Attorney General to provide certain other information, not including the semi-annual report, to the Intelligence Committees "and to the Committees on the Judiciary of the House of Representatives and the Senate." We note that Section 502 of FISA, which was enacted by the USA-Patriot Act, makes the same distinction between the Intelligence and Judiciary Committees. In accord with that distinction, as far as we can establish, Section 108(a) and its counterparts have, since being enacted, been interpreted by both the Department and by Congress to require that the Department provide the full semi-annual report only to the Intelligence Committees of the House and Senate. We submitted our latest such report to the two Intelligence Committees in April 2001, and we would refer you to those Committees on the issue you have raised.

14. **The redacted Field Guidance does not discuss the authority to conduct FISA electronic surveillance and searches when "a significant" purpose is to obtain foreign intelligence information. Please explain how the Department will determine whether to use FISA, rather than criminal law enforcement procedures, for electronic surveillance or search in a case that is being actively considered by the Department for criminal prosecution.**

Answer: The Department is currently in the process of reevaluating its July 1995

intelligence sharing procedures, which govern coordination between intelligence and law enforcement components within the Department, in light of the new legislation. We will, of course, notify the Foreign Intelligence Surveillance Court before implementing any new procedures in matters within the Court's jurisdiction.

15. **FISA requires the approval of the Attorney General or Deputy Attorney General for every electronic surveillance and search under the Act. Under the new law the Director of Central Intelligence has responsibilities for FISA requirements, priorities, and dissemination for foreign intelligence purposes. Please provide information on (a) how those responsibilities will be exercised consistently with the responsibilities of the Attorney General and the FBI for the use of FISA for counterintelligence and law enforcement within the United States; (b) how the DCI will determine the priority for using available FISA capability against organization or governments for law enforcement or counterintelligence purposes in the United States; and (c) how the DCI will determine who will be first in line to get the information for law enforcement or counterintelligence purposes?**

Answer:
(A) and (B) Section 901 of USA-PATRIOT Act does not give the DCI general authority to direct FISA operations and does not purport to affect section 103(d) of the National Security Act (50 U.S.C. 403-3(d)), which proscribes any "police, subpoena, or law enforcement powers or internal security functions" for the CIA. We do not, in that context, believe that section 901 gives the DCI authority to determine what individual FISA operations shall be initiated or terminated and so do not expect that section 901 will affect the ability of the Attorney General and the Director of the FBI to use FISA in accordance with their authorities.

Rather, we interpret section 901 to enable the DCI to consider and include, in his present and well-established levying of general intelligence requirements and priorities upon the Intelligence Community, foreign intelligence collected by FBI and other agencies. The value of foreign intelligence potentially to be collected through a FISA search or surveillance is an important consideration in the determination by the Attorney General and the Director of the FBI in whether to initiate, continue, or terminate a FISA operation conducted by the FBI. The DCI's determination of the value of that foreign intelligence has been, and will under Section 901 continue to be, an important part of their decision-making.

(C) We do not read Section 901 as granting the DCI the authority to "determine" who will get information derived from FISA. Rather, that section states that the DCI is to "provide assistance to the Attorney General" to ensure that information from FISA operations is disseminated effectively for foreign intelligence purposes. We nonetheless recognize that the DCI and CIA have well-established, and effective, means for the disseminating intelligence within the Federal Government and expect to rely upon their guidance in

establishing the mechanism anticipated in Section 901.

16. **The redacted Field Guidance does not discuss the roving surveillance authority under FISA. Does the Department intend that such roving FISA surveillance will be conducted only when the target's presence at the place where, or use of the facility at which, the electronic surveillance is to be directed has been ascertained by the person implementing the order and that the electronic surveillance will be directed only at the communications of the target? If not, please explain how the Department will ensure that the communications of persons who are not targets will not be intercepted.**

Answer: Under section 105 of FISA (50 U.S.C. 1805), the Foreign Intelligence Surveillance Court issues an order specifying the target (if known) of electronic surveillance and the specific means by which that surveillance will be effected. Nothing in Section 206 of the USA-PATRIOT Act changes the specificity of the target or the specific means of surveillance, or authorizes the Government to conduct surveillance of another target or through another means. Rather, Section 206 enables the Court, if it finds that the actions of the target may thwart the identification of a communications carrier, landlord, custodian, or other entity or person in a position to help accomplish the specific type of surveillance it has authorized, to issue a generic order directing assistance in accomplishing that specific type of surveillance against that specific, named target. If, for example, the Court finds that a terrorist might "throw" a cell phone, it may authorize the Government to serve a generic order of assistance for that type of surveillance of that terrorist on his new cell phone.

17. **The redacted Field Guidance does not discuss the provision on access to records and other items under FISA. This provision does not appear expressly supercede other Federal laws protecting specific types of records. Does the Department agree that this provision does not authorize access to records that are protected by other Federal law governing access to the records for intelligence or law enforcement purposes, such as the laws governing access to income tax or census records?**

Answer: The Department does not read Section 215 of the USA-PATRIOT Act as superseding any specific, substantive federal prohibition on such access. Rather, we read Section 215 as providing a procedure by which the Government may, subject to several stated limitations in that section and to other provisions of federal law, petition the Foreign Intelligence Surveillance Court (FISC) for access to "tangible things."