



UNCLASSIFIED

**NATIONAL SECURITY AGENCY  
CENTRAL SECURITY SERVICE**  
FORT GEORGE G. MEADE, MARYLAND 20755-6000

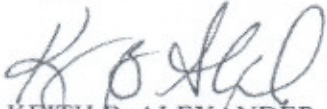
19 December 2006

Honorable Arlen Specter  
Chairman  
Committee on the Judiciary  
United States Senate  
224 Dirksen Senate Office Building  
Washington, DC 20510

Dear Mr. Chairman:

Enclosed please find responses to your 6 September 2006 letter regarding follow-up questions from my testimony at the "FISA for the 21<sup>st</sup> Century" hearing.

If you have any questions, please call me or Michael Lawrence, Director of Legislative Affairs.

*VIR*  
  
KEITH B. ALEXANDER  
Lieutenant General, U.S. Army  
Director, NSA

Encl:  
a/s

UNCLASSIFIED

**Senator Arlen Specter**  
**FISA for the 21<sup>st</sup> Century**  
**Wednesday, July 26, 2006**  
**Questions for Lt. General Keith B. Alexander**

1. Not only has the FISA Court been able to maintain its secrecy where both the Executive and Legislative branches have allowed leaks, but they are in the best position to weigh and balance the nature of the threat, the scope of the program, how many people are being intercepted, what is being done with the information, what is being done on minimization, how successful the program has been, if any projected terrorist threats have been thwarted, and all factors relating to the specifics on the program. Do you believe that the best solution to the possible problem that the president may lack the authority to conduct warrantless wiretaps is to submit the program to the FISA Court of Review and allow them to determine the constitutionality of the program?

ANSWER: (U) No. The Foreign Intelligence Surveillance Court of Review (“the Court of Review”) is an Article III court of limited jurisdiction. The Court of Review does not—and cannot, consistent with the limitations of Article III—issue opinions beyond its statutory authorization. At present, the Court of Review has jurisdiction only with respect to orders of the Foreign Intelligence Surveillance Court *denying* applications by the Government to conduct surveillance pursuant to FISA. *See* 50 U.S.C. § 1803(a), (b). With respect to legislative efforts to change the Court of Review’s jurisdiction, S. 3931 would not alter the jurisdiction of the Court of Review in any relevant respect.

- 2a. Technology has changed tremendously since 1978. What are some of the technological hurdles that make FISA obsolete today?

ANSWER: (U) A full explanation of the technological changes that have impacted the operation of foreign intelligence operations conducted under FISA would require a discussion of highly classified and sensitive information, which is inappropriate for this forum. In short, there has been a radical transformation since 1978 of the means by which the world transmits communications. When FISA was enacted into law in 1978, almost all transoceanic communications into and out of the United States were carried by satellite and those communications were, for the most part, intentionally omitted from the scope of FISA, consistent with FISA’s focus upon regulating the collection of foreign intelligence from domestic communications of United States persons. Congress could not have anticipated the revolution in telecommunications technology that would establish global, high-speed, fiber-optic networks that would fundamentally alter how communications are transmitted. Nor could Congress have anticipated the stunning innovations in wireless technology, or the explosion of the volume of communications, that have occurred in recent decades. Unpredicted advances in the development and deployment of new technologies, rather than a considered judgment by Congress, has resulted in the considerable expansion of the reach of FISA to additional technologies and communications beyond the statute’s original focus on domestic communications.

2b. Do you agree with how S. 2453 deals with emerging technological issues?<sup>1</sup>

ANSWER: (U) Yes. FISA should be amended so that it is technology-neutral. This would return it to what we believe was its original purpose of protecting the privacy of persons in the United States. The revolution in telecommunications technology has extended the impact of the FISA regime far beyond what Congress could ever have anticipated in 1978. At present the requirement for a court order depends in part upon both the location at which surveillance is conducted and the particular communications technology employed. S. 2453 would return FISA to what we believe was its original purpose of protecting the privacy of persons in the United States.

2c. Is it feasible for the FISA Court to make the type of determinations and issue the type of program-wide warrants that the bill envisions?

ANSWER: (U) Yes. The judges of the Foreign Intelligence Surveillance Court are highly experienced with the issues implicated by electronic surveillance conducted for the purpose of collecting foreign intelligence. In addition, many of the requirements for approving an electronic surveillance program are very similar to those that FISC judges have been making for years in authorizing electronic surveillance under FISA. Indeed, many of the “necessary findings” set forth in Section 6 of the bills, including S. 2453 and S. 3931, that the FISC would have to make before authorizing programmatic surveillance are similar to those contained in section 105(a) of FISA, 50 U.S.C. § 1805(a).

3. What suggestions do you have to improve my legislation?

ANSWER: (U) All suggestions NSA had for improving the draft legislation have already been provided in the informal Administration process of consultation and providing technical assistance. We look forward to working further with you and Congress as this bill moves through the legislative process. FISA reform is extremely important to the security of the country.

4. Could the Foreign Intelligence Surveillance Court (FISC) authorize a broad collection whereby communications are intercepted when the connection to terrorism is very attenuated or would that potentially violate the Fourth Amendment?

ANSWER: (U) NSA is not in a position to speculate on what actions the FISC might take in a particular case. Of course, all surveillance conducted under FISA must be consistent with the Fourth Amendment’s overriding requirement of reasonableness.

5. Was the Court of Review correct when it said that FISA cannot encroach on the President's constitutional authority?

---

<sup>1</sup> NSA notes that the proposed language of S. 2453 continues to be modified. At present, the Senate’s FISA modernization proposal that most closely resembles S. 2453 is S. 3931, the Terrorist Surveillance Act of 2006, as introduced. In most cases, the answers provided herein are responsive to the questions that remain relevant in S. 3931; i.e., where the language in S. 3931 does not substantively change the context of the question. A note has been made to indicate those questions where the significant changes in S. 3931 make the question inapplicable.

ANSWER: (U) Yes. Although the Department of Justice is better suited to answer constitutional law questions, the general point that legislation cannot override the Constitution is correct. Congress cannot by statute take away from the President authority that the Constitution vests in him.

5a. If that is so, does repealing the so-called exclusivity provision do more than make clear that Congress does not wish to provoke a constitutional clash?

ANSWER: (U) The Department of Justice is better suited to answer this question. Nevertheless, I would say that repealing the so-called “exclusive means” provision would make clear that Congress is not interested in provoking a conflict between the branches.

5b. Aside from the constitutional law, is it good policy to interfere with the President's ability to detect and prevent terrorist plots of a declared enemy?

ANSWER: (U) It is, of course, never good policy to interfere with the Nation’s ability to detect and to prevent terrorist plots. Recent events in Britain remind us that, five years after al Qaeda succeeded in launching the single most deadly foreign attack on American soil in history, we continue to confront a determined and deadly enemy that is dedicated to launching further catastrophic attacks against America. We act at our peril if we do not do everything in our power to detect and prevent such plots.

6. In your opinion, would the President continue the Terrorist Surveillance Program if the Foreign Intelligence Surveillance Court or the Court of Review concluded that the program is unconstitutional?

ANSWER: (U) I cannot, of course, speak for the President on what he might do if the FISC or the Court of Review concluded that the Program is unconstitutional. That said, I am confident that the Terrorist Surveillance Program is lawful and that the courts will come to the same conclusion.

**Senator Charles E. Schumer**  
**FISA for the 21<sup>st</sup> Century**  
**Wednesday, July 26, 2006**  
**Questions for Lt. General Keith B. Alexander**

1. On July 13, Senator Specter announced that he had reached a deal with the White House on his legislation to authorize the Terrorist Surveillance Program and re-write much of the Foreign Intelligence Surveillance Act (FISA). This was just two weeks after the Supreme Court's decision in *Hamdan*, which many have characterized as a rebuke of the Administration's legal defense of the President's warrantless surveillance program.
  - 1a. Do you continue to believe that the NSA Surveillance Program is legal and Constitutional and that it would survive any legal challenge in the FISA Court?

ANSWER: (U) NSA believes that the Terrorist Surveillance Program is lawful, and that the Foreign Intelligence Surveillance Court would uphold the legality of the Program. As Assistant Attorney General Moschella explained in his detailed response to your June 30th letter, it is the considered legal judgment of the Executive Branch that the Supreme Court's decision in *Hamdan v. Rumsfeld* does not affect the analysis set forth in the Department's January 19th *Legal Authorities* paper outlining the legal basis for the Terrorist Surveillance Program. As the Moschella letter explains, there are many reasons to support that conclusion, but at bottom, the relevant statutory scheme at issue in *Hamdan* is fundamentally different from the one implicated by the Terrorist Surveillance Program. FISA expressly contemplates that Congress may authorize electronic surveillance through a subsequent statute without amending or repealing FISA. See 50 U.S.C. § 1809(a)(1) (prohibiting electronic surveillance "except as authorized by statute"). The primary provision at issue in *Hamdan*, Article 21 of the Uniform Code of Military Justice ("UCMJ"), has no analogous provision. Moreover, the Supreme Court recognized in *Hamdi v. Rumsfeld*, 542 U.S. 519 (2004), that the Authorization for Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (Sept. 18, 2001), satisfies a statute similar to FISA prohibiting detention of U.S. citizens "exception pursuant to an Act of Congress," 18 U.S.C. § 4001(a). Because the Terrorist Surveillance Program implicates a statutory regime analogous to the one at issue in *Hamdi*, we believe that the reasoning of that decision is far more relevant to the Program than *Hamdan*.

- 1b. If the administration has "the authority, both from the Constitution and the Congress, to undertake this vital program," as President Bush asserted in January, what need is there to legislate on this issue from your perspective?

ANSWER: (U) As stated in the Department of Justice's *Legal Authorities* paper, the Executive Branch has the statutory and the constitutional authority to implement the Terrorist Surveillance Program. Nevertheless, additional legislation could be very helpful by providing additional authority for the Terrorist Surveillance Program and by modernizing FISA to confront the new threats and technologies of the 21<sup>st</sup> Century.

- 1c. Would you prefer that Congress not legislate in this area at all?

ANSWER: (U) No. As indicated above, the Executive Branch wants to work with Congress on electronic surveillance issues, including legislation addressing the Terrorist Surveillance Program.

- 1d. Did the Supreme Court's recent ruling in *Hamdan* play any role in the Administration's decision to support Senator Specter's legislation?

ANSWER: (U) No. The Executive Branch supports Senator Specter's bill, S. 2453, because it is a sound proposal to allow the FISC to approve programmatic electronic surveillance and to modernize FISA, while better protecting the privacy of United States persons.

2. Senator Specter has characterized his bill as simply allowing the Court to decide the Constitutionality of the program, including whether the President has the authority to authorize this surveillance. It has been said that if kept in its precise current form, the President will submit the program to the FISA Court. Why doesn't the Administration just submit the program to the FISA Court now, without any legislation?

ANSWER: (U) Traditional FISA procedures do not allow the speed and agility that makes the Terrorist Surveillance Program such an important early-warning system. Legal options, however, are always being evaluated.

3. If the Specter bill is passed in its current form, what signing statement do you anticipate the President issuing in connection with it?

ANSWER: (U) NSA is not in a position to answer this question.

4. If the Specter bill is passed in its current form, and the Administration then voluntarily submitted the program to the FISC, would the Administration argue that the Specter bill authorized the NSA's Terrorist Surveillance Program?

ANSWER: (U) NSA is not in a position to answer this question.

5. Do you believe that the portion of the Specter bill that allows the President to submit the NSA surveillance program to the FISA Court is constitutional? Specifically, do you believe this provision does not run afoul of the constitutional proscription against advisory opinions?

ANSWER: (U) NSA is not in a position to answer this question.

6. The Specter bill provides that any cases pending right now – upon application by the Attorney General – must be transferred to the FISA Court of Review. The bill also provides that the decision of that FISA Court “shall be subject to certiorari review in the United States Supreme Court.”



6a. Is it your understanding that one who is challenging a FISA Court decision favorable to the government may obtain review before the Supreme Court under the bill?

ANSWER: (U) NSA is not in a position to answer this question.

6b. What are the arguments against allowing the constitutional review in a traditional Federal District Court, with expedited review to the Supreme Court, so long as the court applies the procedures and standards of the Classified Information Procedures Act?

ANSWER: (U) The FISC is better suited than ordinary district courts to deal with this area of law both because of its experience in that area of law and because it has the facilities and experience required to handle highly classified material.

7. During his February appearance before the Committee, Senator Biden asked Attorney General Gonzales what harm had been caused by public disclosure of the warrantless surveillance program. He responded: "You would assume that the enemy is presuming we are engaged in some kind of surveillance. But if they're not reminded about it all the time in the newspapers and in stories, they sometimes forget." When I asked him the same question in July, he deferred to the intelligence community.

7a. Do you have a better answer as to how the disclosure that wiretapping is going on harmed national security?

ANSWER: (U) Disclosure of the Terrorist Surveillance Program puts at risk efforts by the U.S. Government to prevent catastrophic al Qaeda-sponsored attacks within the United States. Even the smallest reduction in the effectiveness of the Program could be catastrophic in an environment in which we cannot afford to miss one plot, one event, one individual, or one movement. These unauthorized disclosures also have a chilling effect on cooperation, affecting both friendly governments and individual clandestine sources. To put it starkly, if we cannot be trusted to keep our own secrets, why should others share sensitive information with us? Finally, foreign intelligence services and non-state terrorist groups capitalize on this public hemorrhage of U.S. secrets, which becomes a "bonus," enriching the unclassified open source collection activities many of our opponents already perform.

7b. To your knowledge have any officials in the intelligence community had direct discussions with Attorney General Gonzales or officials in his Department about how disclosure of the program harmed national security? If so, what was said?

ANSWER: (U) Neither I nor other officials in the Intelligence Community can reveal the internal deliberations of the Executive Branch or the content of our confidential discussions with the Attorney General.

8. Do you have legal or constitutional concerns about the use of warrantless physical searches in the United States?

ANSWER: (U) No. NSA is confident that any such activities would be conducted only as consistent with the laws of the United States, including the Constitution. We are not, however, in a position to either confirm or deny any asserted intelligence activities.

9. To your knowledge, has the Administration ever used its commander-in-chief powers or the AUMF to justify warrantless physical searches?

ANSWER: (U) NSA is not in a position to confirm or deny any asserted intelligence activities. Our inability to discuss such asserted programs should not be taken as an indication that such activities exist.



**Senator Dianne Feinstein  
FISA for the 21<sup>st</sup> Century  
Wednesday, July 26, 2006  
Questions for Lt. General Keith B. Alexander**

**Background.** Several of us in Congress – and especially those of us serving on the Intelligence Committees – were surprised and disappointed that we had to learn of the so-called Terrorist Surveillance Program from the *New York Times*. Since then, we have read reports about other programs as well.

A May 12, 2006 *USA Today* story, reporting on the NSA's apparent collection of millions or even billions of telephone records from major carriers, has been denied by some carriers but not others. Last week, it was revealed that Republican House Intelligence Chairman Hoekstra had sent a letter to the Administration complaining of another program that had not been disclosed to his committee. And in earlier testimony, the Administration has alluded to the possibility, but did not confirm, that other intelligence programs could exist.

- Are there any intelligence programs carried out by your agencies, or otherwise within the intelligence community that you know of, that have not been briefed to the Congressional intelligence committees?

ANSWER: (U) As Director of the National Security Agency, I can only speak for NSA. I assure you that NSA takes its congressional reporting obligations extremely seriously. The National Security Act of 1947 contemplates that the Intelligence Committees of both Houses would be appropriately notified of any such intelligence programs that exist, and the Act specifically contemplates more limited disclosure in the case of exceptionally sensitive matters. Title 50 of the U.S. Code provides that the Director of National Intelligence and the heads of all departments, agencies, and other entities of the Government involved in intelligence activities shall keep the Intelligence Committees fully and currently informed of intelligence activities “[t]o the extent consistent with due regard for the protection from unauthorized disclosure of classified information relating to sensitive intelligence sources and methods or other exceptionally sensitive matters.” 50 U.S.C. §§ 413a(a), 413b(b). It has for decades been the practice of both Democratic and Republican administrations to inform only the Chair and Ranking Members of the Intelligence Committees about exceptionally sensitive matters. The Congressional Research Service has acknowledged that the leaders of the Intelligence Committees “over time have accepted the executive branch practice of limiting notification of intelligence activities in some cases to either the Gang of Eight, or to the chairmen and ranking members of the intelligence committees.” See Alfred Cumming, *Statutory Procedures Under Which Congress is to be Informed of U.S. Intelligence Activities, Including Covert Actions*, Congressional Research Service Memorandum at 10 (Jan. 18, 2006).

- Did anyone in the Administration offer, grant or otherwise provide in any way some sort of promise of immunity or offer of protection against civil or criminal liability to

UNCLASSIFIED

telecommunications or internet service provider or financial entities or any other company for their cooperation in any of the surveillance programs? If yes, under what legal authority?

ANSWER: (U) Operational information about the Terrorist Surveillance Program is highly classified and exceptionally sensitive. Publicly revealing information about the operational details of the Program could compromise its value and facilitate terrorists' attempts to evade it. Accordingly, we cannot confirm or deny operational details of the Program in this setting. As you are aware, the operational details of the Program have been and continue to be reviewed by the full intelligence committees and, in certain circumstances, congressional leadership.

UNCLASSIFIED

**Senator Edward M. Kennedy**  
**FISA for the 21<sup>st</sup> Century**  
**Wednesday, July 26, 2006**  
**Questions for Lt. General Keith B. Alexander**

1. In a White House press briefing on December 19, 2005, Attorney General Gonzales said that the standard for beginning surveillance on an individual under the NSA warrantless wiretapping program is “a *reasonable basis* to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda.” Similarly, in a session with *The San Diego Union-Tribune*, published on February 5, 2006, General Hayden said that the constitutional standard under the Fourth Amendment is “*reasonableness*,” ignoring the probable cause provision of the Fourth Amendment.

However, as General Hayden told the Senate Judiciary Committee on July 26, 2006, “There is a *probable cause* standard, before any communication is intercepted, that one or both communicants is, again, to a probable cause standard, associated with al Qaeda.”

- 1a. Is the standard used by the NSA reasonableness or probable cause, in determining the targets for wiretapping under the NSA’s warrantless wiretapping program? Has the standard ever changed from “probable cause” at any time, for any reasonable period, since September 11<sup>th</sup>?

ANSWER: (U) The Department of Justice is in a better position to discuss the “probable cause” standard. Nevertheless, the Terrorist Surveillance Program is narrowly tailored to target for interception only communications where one party is outside the United States and there are reasonable grounds to believe that at least one party is a member or agent of al Qaeda or an affiliated terrorist organization. The Program has consistently employed this standard. The “reasonable grounds to believe” standard is synonymous with “probable cause.” *See, e.g., Maryland v. Pringle*, 540 U.S. 366, 371 (2003) (“We have stated . . . that “[t]he substance of all the definitions of probable cause is a reasonable ground for belief of guilt.”) (internal quotation omitted).

2. The bill negotiated between Senator Specter and the Administration would allow authorization of a spying program targeted not just at members of al Qaeda but at anyone “reasonably believed to have communication with or be associated with” *any* foreign powers or their agents engaged in terrorism preparations. This broad standard could sweep in thousands of innocent Americans who are unaware that someone in the federal government has determined that they are “associated with” a person the government considers to be a terrorist.

Question:

- 2a. What is the justification for a standard that is even broader than the current standard, which requires probable cause that one person involved in the communication is directly “affiliated with al Qaeda” or “associated with al Qaeda” [The standard most recently

articulated by General Hayden at the July 26, 2006, hearing before the Senate Judiciary Committee]?

ANSWER: (U) The United States faces a flexible, secretive, decentralized, and constantly evolving global network of terrorist cells. The need for an agile surveillance system is at a premium because our adversaries in the War on Terror seek to inflict massive casualties through another catastrophic attack on our homeland.

2b. What would be the basis and legal standard to conclude that a U.S. person is “associated with” al Qaeda or an organization determined to be affiliated with al Qaeda under the proposed legislation?

ANSWER: (U) The professional intelligence officers at the National Security Agency, who are experts on al Qaeda and its tactics, including its use of communication systems, with the assistance of other elements of the Intelligence Community and subject to appropriate and vigorous oversight by the NSA Inspector General and General Counsel, among others, would rely upon the best available intelligence information to determine whether there are reasonable grounds to believe that a party to an international communication is affiliated with al Qaeda.

3. In December 2005, at a White House press briefing, General Hayden said that the NSA warrantless wiretapping program targeting communications that involve al Qaeda, with one end inside the United States, had been successful in detecting and preventing terrorist attacks. He also said that the program deals only with international calls with a time period much shorter than is typical under the Foreign Intelligence Surveillance Act.

When asked about the inadequacies of FISA, which led to the creation of the domestic spying program, General Hayden said that the “whole key here is agility... [and] the intrusion into privacy is significantly less. It’s only international calls,” and the time period for surveillance is shorter than that is generally authorized under the Foreign Intelligence Surveillance Act. Attorney General Gonzales reiterated the statement that the program was limited to those with ties to al Qaeda.

In a session with the *San Diego Union-Tribune*, General Hayden said that the publicly acknowledged program is “limited” and “focused,” and has been “effective.”

At the Senate Judiciary Committee hearing on July 26, 2006, Mr. Bradbury stated that the program involves “monitoring of international communications into and out of the United States where there are reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliate terrorist organization.”

The program described in the bill negotiated by the Administration and Senator Specter is significantly broader than the program General Hayden said had been successful in detecting and preventing attacks. The bill would allow authorization of a spying program targeted not just at members of al Qaeda but at anyone

“reasonably believed to have communication with or be associated with” *any* foreign powers or their agents engaged in terrorism preparations. This broad standard could sweep in thousands of innocent Americans who are unaware that they are “associated with” a person the government considers to be a terrorist.

General Hayden has also repeatedly stated that the targets for the wiretapping are approved by “shift supervisors,” whom he later characterized as “senior executives.” Yet, this bill authorizes the Attorney General to delegate his authority to anyone he wishes, instead of limiting the delegation to senior officials.

Questions: Members of the Administration have repeatedly claimed that the publicly announced program has saved an untold number of American lives.

3a. Why did the Administration insist on a bill that would allow the authorization of a program that spies on even more Americans?

ANSWER: (U) The Terrorist Surveillance Program *does not* involve “domestic spying.” As the Executive Branch has stated on a number of occasions, the Program targets communications where one party is outside the United States and there are reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated terrorist organization. Under the Program, decisions about what communications to intercept are made by professional intelligence officers at the National Security Agency who are experts on al Qaeda and its tactics, including its use of communication systems. Relying upon the best available intelligence and subject to appropriate and vigorous oversight by the NSA Inspector General and General Counsel, among others, the NSA determines whether one party is outside the United States and whether there are reasonable grounds to believe that at least one of the parties to the communication is a member of al Qaeda or an affiliated terrorist program. Procedures are also in place under the Program to protect U.S. privacy rights, including applicable procedures required by Executive Order 12333 and approved by the Attorney General, which govern acquisition, retention, and dissemination of information relating to United States persons. The NSA takes very seriously the need to protect the privacy of United States persons. S. 2453 provides additional authority to help protect the Nation in a way that also protects privacy interests of Americans.

3b. Is this just another attempt to expand Executive authority even further, or does the Administration have a specific, documented need to spy on far larger numbers of innocent Americans than are at risk under the current program?

ANSWER: (U) The Executive Branch has no need to spy and no interest in spying on any innocent Americans. The NSA supports modernizing FISA to address the threat confronted by the United States and providing additional support for the Terrorist Surveillance Program to protect American lives and to enhance the communications privacy of United States persons. Recent events in Britain remind us that, five years after al Qaeda succeeded in launching the single most deadly foreign attack on American soil in history, we continue to confront a

determined and deadly enemy that is dedicated to launching further catastrophic attacks against America. We act at our peril if we do not do everything in our power to detect and prevent such plots. Although FISA remains a vital tool in the War on Terror, the Terrorist Surveillance Program provides an advantage in terms of speed and agility that is critical to successful intelligence collection against a flexible, secretive, diffused, and constantly evolving global network of terrorist cells. The Executive Branch takes very seriously the need to protect Americans from terrorist threats consistent with the protection of civil liberties. To that end, electronic surveillance is conducted in accordance with the law.

3c. What are the Administration's justifications for such a broad program that far exceed the program described publicly by each of you in past statements and in testimony before this Committee?

ANSWER: (U) There is no reason to believe that either S. 2453 or S. 3931 would authorize programs that "far exceed" the Terrorist Surveillance Program in size and scope, since any such program would still have to meet the Fourth Amendment's reasonableness requirement. The Executive Branch takes very seriously the need to protect Americans from terrorist threats consistent with the protection of civil liberties. Electronic surveillance is conducted with Congress's oversight and in accordance with the law.

4. At the July 26, 2006, Senate Judiciary Committee hearing, Mr. Bradbury described the NSA warrantless wiretapping program as "monitoring of international communications into and out of the United States where there are reasonable grounds to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliate terrorist organization."

Question:

4a. What is the legal definition of an "affiliate terrorist organization"?

ANSWER: (U) Whether a particular group is an "affiliate terrorist organization" of al Qaeda is a factual matter determined by experts in the Intelligence Community.

4b. Who makes the determination that an organization is one that is an "affiliate terrorist organization" to al Qaeda?

ANSWER: (U) Experts in the Intelligence Community, relying upon the best available intelligence information, their expertise, and their judgment, determine which groups are "affiliate terrorist organization[s]" of al Qaeda.

4c. What are the criteria used?

ANSWER: (U) The criteria used to determine whether a group is affiliated with al Qaeda are developed by the Intelligence Community based on the best information available about the characteristics and behavior of terrorist groups.

4d. How quickly is such a determination made?

ANSWER: (U) The Intelligence Community endeavors to make an accurate decision regarding whether a group is affiliated with al Qaeda as quickly as possible, based upon the best available information.

5. The Intelligence Authorization Act for fiscal year 2000 included a provision requiring a report to Congress from the intelligence community on the legal standards used by agencies in conducting signals intelligence, including electronic surveillance. Congress wisely saw the need to require legal justification from the intelligence community on any program affecting the privacy interests of Americans. The report was submitted before 9/11. In that report, the NSA said, “in order to conduct electronic surveillance against a U.S. person located within the United States, FISA requires the intelligence agency to obtain a court order from the Foreign Intelligence Surveillance Court.” We must guarantee the same oversight in any new legislation.

Question:

5a. Will the Administration agree to report on the legal standards being used now? Obviously, the standards provided to Congress in 2000 have become outdated and, perhaps, obsolete.

ANSWER: (U) The Executive Branch has provided the Committee with extensive information regarding the legal standards currently applicable to foreign intelligence surveillance. On January 19, 2006, the Department of Justice released 42-page paper setting forth the legal rationale underlying the Terrorist Surveillance Program and explaining, consistent with the public nature of that document, the standards used in the Program. Since that time, officers of the NSA and the Department of Justice have appeared in numerous public and classified congressional hearings on these legal standards, and have answered hundreds of questions for the record about the Terrorist Surveillance Program. In addition, every member of both of the Intelligence Committees has been authorized to be briefed about the Terrorist Surveillance Program and nearly all have availed themselves of this opportunity.

6. In a White House press briefing on December 19, 2005, General Hayden said that shift supervisors determine individual targets for warrantless wiretapping; in February 2006, General Hayden said that “senior executives” make these decisions.

Questions:

6a. What specific level of government official is making the determination that there is either “reasonableness” or “probable cause” to bring a person into surveillance under this program?

ANSWER: (U) A select group of senior officers at NSA, who are experts on counterterrorism generally and al Qaeda and its communications tactics specifically, are authorized to approve surveillance under the Terrorist Surveillance Program. All authorizations to conduct surveillance under the Program are subject to rigorous oversight by the Office of the Inspector General and



the Office of the General Counsel of the NSA, as well as by attorneys from the Department of Justice.

6b. What legal training do these officials have, if any?

ANSWER: (U) Although the NSA personnel making the initial determinations to conduct electronic surveillance do not have formal legal training, the determination itself is premised on the common-sense judgments of reasonable and prudent people. Indeed, the federal Courts have consistently held that the probable cause standard is a practical, nontechnical concept. *See, e.g., Maryland v. Pringle*, 540 U.S. 366, 371 (2003); *Illinois v. Gates*, 462 U.S. 213, 235-36 (1983). Probable cause refers simply to reasonable grounds for a belief that one holds based on the factual and practical considerations of everyday life on which reasonable and prudent persons act. *Pringle*, 540 U.S. at 366.

(U) These officers are an integral part of the rigorous review process NSA has instituted as part of the Terrorist Surveillance Program to protect the privacy of United States persons. Relying upon the best available intelligence and their training and experience regarding counterterrorism, these officers—before ordering the interception of certain international communications—must determine whether there is probable cause (“reasonable grounds”) to believe that at least one of the parties to the communication is a member or agent of al Qaeda or an affiliated terrorist organization.

(U) As I have noted previously, the Terrorist Surveillance Program of course is subject to intense legal oversight, within the NSA and by other elements or agencies within the Executive Branch. The oversight process includes review at the National Security Agency (by both the Office of General Counsel and Office of Inspector General) and the Department of Justice.

6c. What are their qualifications to make the decision to target an individual for surveillance on U.S. soil, a decision that is required to be made by a FISA Court judge under existing law?

ANSWER: (U) We disagree with the assertion that “existing law” always requires a judge of the FISC to make the determination whether to authorize foreign intelligence surveillance involving a person within the United States. As set forth in greater detail in the Department of Justice’s *Legal Authorities Supporting the Activities of the National Security Agency Described by the President* (Jan. 19, 2006) (“*Legal Authorities*”), the courts have long recognized that the President has inherent authority under the Constitution to conduct electronic surveillance for the purposes of collecting foreign intelligence information without prior judicial approval. Congress has confirmed and supplemented that authority through the September 18, 2001 Authorization for the Use of Military Force (“Force Resolution”). Decisions about what communications to intercept are made by professional intelligence officers who are experts on al Qaeda and its tactics, including its use of communications systems. These experts have years of training and experience in the field of counterterrorism. Relying on the best available intelligence and subject to appropriate and rigorous oversight by the NSA Inspector General and General Counsel, among others, these officers determine whether there is probable cause to believe that one of the parties to a communication is a member or agent of al Qaeda or an affiliated terrorist organization.

7. At the July 26, 2006, Senate Judiciary Committee hearing, General Hayden said, “[T]he Government looks to four factors in assessing whether or not a court order is required before NSA can lawfully intercept a communication...those factors are: who is the target, where is the target, how do we intercept the communication, and where do we intercept the communication.”

Questions:

- 7a. Who at the NSA assesses each of these four factors? If you are unable to name specific people, what level of government official makes this assessment?

ANSWER: (U) My understanding is that the above-quoted statement from General Hayden’s testimony at the July 26 hearing did not in any way concern the Terrorist Surveillance Program. Rather, his statement concerning the ‘who, what, where, and how’ of intercepting an electronic communication is addressed to the determinations that must be made regarding whether FISA even applies to a particular communication. General Hayden’s statement is true generally for all NSA intelligence collection activities, and has been true for the 28 years FISA has been in effect. The four issues must be considered because the manner in which FISA defines the term “electronic surveillance” is in part dependent on factors that those questions address.

(U) While there is no single person whose job it is to assess these factors, the Office of General Counsel provides legal advice to NSA employees, including training specifically concerning the applicability of the FISA, and is available to provide legal advice in a given situation to NSA officials concerning the applicability of the statute. Sometimes it is quite clear to an individual responsible for initiating surveillance that no court order is required under the particular circumstances contemplated, such as when NSA wants to conduct surveillance of a foreign target located overseas using a surveillance technique accomplished entirely overseas. At other times, it is clear that FISA does require a court order, such as when the government seeks to acquire the contents of a wire communication sent by or intended to be received by a particular known U.S. person in the United States by targeting that person.

- 7b. What legal training do these staff members have, if any?

ANSWER: (U) Please see our responses to questions 6b, 6c, and 7a, above.

- 7c. What are their qualifications to make this determination?

ANSWER: (U) Please see our responses to questions 6b, 6c, and 7a, above.

8. In response to Senator Specter’s question about whether or not it is “impossible or impractical to get an individualized warrant when the caller is outside of the United States, not knowing whether the recipient will be inside the United States,” you said, “it would be impractical because we don't know what the foreign to U.S. number could possibly be.” However, FISA allows you to begin tapping a source immediately and continuously for up to 72 hours while you pursue a warrant. This can be done entirely at the discretion of the Attorney General, as long as he makes a good-faith effort to “reasonably determine[.]” that “an emergency situation

exists” and that “the factual basis for the issuance of an order . . . exists.” 50 U.S.C. § 1805.

You made the same argument in response to Senator Feinstein’s question about obtaining FISA warrants under the current law to execute the NSA surveillance program, arguing that “it would require us to get a FISA on every foreign one in advance because we do not know who they are calling until it has happened,” again ignoring the 72-hour grace period under the current law.

Questions:

- 8a. Given that current law allows for the 72-hour grace period for obtaining a warrant, why would you have to get those warrants “in advance”? Would you clarify your answer to Senator Feinstein’s question?

ANSWER: (U) Thank you for the opportunity to correct a common misperception about FISA. The emergency authorization provision in FISA, which allows 72 hours of surveillance without obtaining a court order, does not—as many believe—allow the Government to undertake surveillance immediately. Rather, in order to authorize emergency surveillance under FISA, the Attorney General first must personally “determine[] that . . . the factual basis for issuance of an order under [FISA] to approve such surveillance exists.” 50 U.S.C. § 1805(f). For surveillance requested by NSA, that process ordinarily entails review by intelligence officers at the NSA, NSA attorneys, and Department of Justice attorneys, each of whom must be satisfied that the standards have been met before the matter proceeds to the next group for review. In addition, if the Attorney General authorizes emergency surveillance and the FISA court later declines to permit surveillance, the surveillance must cease 72 hours after its initial authorization, and there is a risk that the court would disclose the surveillance publicly. *See id.* § 1806(j). To meet the statutory requirements and to reduce those risks, the Attorney General must ensure that any “emergency” surveillance ultimately will be acceptable to the FISA court, in essence requiring the Attorney General to be certain in advance that the FISC would grant a warrant before even initiating emergency surveillance.

- 8b. If the problem with the current law is an inability for the NSA to process the required number of FISA petitions within the 72-hour window, why not simply amend the statute to extend the grace period? If the grace period were extended to a month, or three months, the NSA could discard useless information and use the ample extra time to apply for warrants to cover any useful information. Why do we need the Chairman’s sweeping overhaul if the actual problem can be solved in a targeted manner?

ANSWER: (U) NSA supports extending the period that surveillance can be conducted before obtaining an order from the FISC, but that alone would not be sufficient to enable the United States to collect foreign intelligence from an agile and flexible enemy. As noted above, modernization of FISA and provisions dealing with programmatic orders are needed to help us detect and to prevent future terrorist attacks by al Qaeda and its affiliates as well as to counter other foreign threats.

8c. If the concern is about the time that it takes for the Attorney General to approve wiretapping under the emergency 72-hour provision, why does it take longer to meet the requirements of FISA (“reasonably determin[ing] that “an emergency situation exists” and that “the factual basis for the issuance of an order...exists”) than the Administration’s standard for the warrantless wiretapping program (“a communication we believe to be affiliated with al Qaeda, associated with al Qaeda, one end of which is in the United States, and we believe at least one end we have a probable cause standard is al Qaeda”)? Could this problem be solved by delegating this responsibility to specified senior officials with legal proficiency in these matters? Or the allocation of additional resources to the FISA Court or the relevant federal agencies gathering intelligence?

ANSWER: (U) By itself, amending FISA to permit a senior official other than the Attorney General to authorize an emergency wiretap would not make FISA suitable to provide the sort of early warning system necessary. Under such a proposal, it would still be necessary for the official first to personally “determine[] that . . . the factual basis for issuance of an order under [FISA] to approve such surveillance exists.” 50 U.S.C. § 1805(f). Because the failure to obtain a court order within 72 hours authorizing the interception would result in the surveillance being stopped and would risk its disclosure, the Executive Branch would still need to follow the existing multi-layered review procedure before any such official would authorize “emergency” surveillance. Under FISA, each statutory requirement must be included in each application to ensure the application is approved. For example, the statute requires that each application contain a statement of facts supporting the application, a certification from a high-ranking official with national security responsibilities, and the signature of the Attorney General. FISA applications are sometimes an inch thick. This proposal would still present the Executive Branch with a bottleneck prior to authorization, and would do nothing to alleviate the bottleneck at the application stage.

(U) For these and other reasons, committing even substantial additional resources within the traditional FISA framework for obtaining orders—while welcome—would not provide the flexibility and agility necessary to allow it to function as an early warning system against attacks by al Qaeda and affiliated terrorist organizations. There are several problems with traditional FISA procedures that cannot be solved simply by allocating additional money to foreign intelligence collection. First, these traditional procedures require individual applications for each target. *See* 50 U.S.C. §§ 1804 & 1805. Second, the tremendous changes in global telecommunications technology since 1978 have resulted in the unintended expansion of the reach of FISA to include international communications that Congress intended to exclude from the scope of the statute. This unintended expansion of FISA’s scope requires the Government and the FISC to devote considerable resources to surveillance that Congress intended not to regulate through FISA. Third, section 104 of FISA, 50 U.S.C. § 1804, currently requires certifications from high-level national security officials and personal approval by the Attorney General of all applications to the Foreign Intelligence Surveillance Court, thus creating “bottlenecks” in the application process that cannot be eliminated simply by appropriating additional funds to foreign intelligence surveillance.

9. The procedures required by FISA are often blamed for the Administration’s difficulties in predicting and responding to 9/11. However, as has been widely reported, the NSA

intercepted statements on September 10<sup>th</sup> referring to the September 11<sup>th</sup> attacks, but these warnings were not translated until September 12<sup>th</sup>—too late to provide any warning of the devastation planned for New York and Washington, DC. In the five years since September 11<sup>th</sup>, the media has continued to report that intelligence agencies, including the NSA, do not have the ability to keep up with the translation demands of the war on terror. At the Senate Judiciary Committee hearing on July 26, 2006, General Hayden acknowledged the translation backlogs and concerns about allocating resources.

Questions:

9a. What are you and others at the NSA doing to hire more translators of Arabic and other languages that are critical to fighting terrorism?

ANSWER: (U) The Global War on Terror and continuing military campaigns have placed an enormous burden on NSA's population of civilian and military language and intelligence analysts. Supplemental funding has helped to expand the contract linguist population in several low-density crisis languages, increase analytic training across the extended SIGINT enterprise, immediately activate a civilian Cryptologic Reserve Program, and significantly expand the Military Reserve program. The Agency continues to need skilled linguists and analysts, and is aggressively pursuing qualified applicants.

9b. Is there currently a backlog in translating intelligence information? If so, what is the average amount of time between an interception that takes place under surveillance and its translation? Do you have a system in place to prioritize translation of critical information? If so, how do you determine which intelligence is more important than other information?

ANSWER: (U) Depending on the source of the information there could be time lags between when it was intercepted and when it was available for a linguist to review at NSA Headquarters. Given the wide differences in targets and the methods of communicating, we cannot give an estimate of an average time lag.

(U) Although we have made significant progress in addressing the problems identified in 2001, the translation backlog is a systemic issue. Terrorist lead information has proliferated since 2001 and, unfortunately, it is a very labor intensive exercise to sift through large volumes of foreign language data and painstakingly attempt to separate the wheat from the chaff. This dilemma is compounded by the fact that the target set has expanded exponentially since 2001 in terms of geographic reach and languages used. Today's backlog is no longer confined to Arabic and its multiple dialects, but also includes a variety of other less commonly taught languages, where linguists eligible for security clearances are in short supply.

9c. If there is a backlog in translation, how does this affect your ability to protect America from future terrorist attacks?

ANSWER: (U) It is important to bear in mind that SIGINT is only one component of America's defense and, given the vague and fragmentary nature of terrorist communications, it is more likely that a combination of intelligence sources will be necessary to prevent a terrorist attack. What SIGINT can do is work hand-in-glove with other intelligence agencies, the military, and

law enforcement to enable key takedowns, so that the details of a plot can be uncovered through interrogation and forensics exploitation. That being said, the translation backlog can prevent the timely delivery of key information to NSA's customers and stall development efforts against new targets.

9d. What resources are required for the NSA to increase its translation efficiency to a level at which translation will not be an impediment to protecting America?

ANSWER: (U) NSA must have a robust hiring and contracting program for GWOT languages, with a particular focus on the identification and recruitment of high-caliber, clearable native speakers, and the agility to adapt to the constantly-changing needs of the terrorist target set. NSA will also need better analytic methods, which we call "Human Language Tools," to help focus efforts on the most lucrative leads, given that it will never be possible to fully exploit all of the material that we have the capacity to collect. Finally, NSA needs a high-quality GWOT language training program to help our current linguists acquire the necessary skills to address this challenging target set.

**Senator Dick Durbin**  
**FISA for the 21<sup>st</sup> Century**  
**Wednesday, July 26, 2006**  
**Questions for Lt. General Keith B. Alexander**

1. It is interesting that 4 ½ pages of your 5-page written statement focus on the Specter bill's change in the definition of electronic surveillance. You clearly believe it is important to make this change in the law to facilitate effective surveillance of terrorists.

When did you become aware of the problem with current law? Do you know why the administration has not previously asked Congress to change the definition of electronic surveillance?

ANSWER: (U) It has long been known that FISA's existing definition of "electronic surveillance" is obsolete and that changes in technology inadvertently are sweeping within the scope of FISA electronic communications that Congress in 1978 had intended to exclude. It was our judgment, however, that disclosing that fact to explain the need to reform the definition of "electronic surveillance" could disclose sensitive intelligence sources and methods. Such disclosures would have posed a serious risk to national security. Numerous unauthorized and harmful disclosures of intelligence activities, including the public disclosure of the Terrorist Surveillance Program, have reduced the risk of additional damage to national security from seeking to amend FISA to solve the inadvertent expansion in FISA's scope since 1978.



**Senator Russell D. Feingold**  
**FISA for the 21<sup>st</sup> Century”**  
**Wednesday, July 26, 2006**  
**Questions for Lt. General Keith B. Alexander**

Following are questions regarding the July 25, 2006, version (marked “JEN06974”) of Senator Specter’s bill, which was originally introduced as S. 2453<sup>2</sup>. Please respond to the greatest degree possible in an unclassified setting, and please endeavor to provide any classified answers at a clearance level that will allow at least some cleared Judiciary Committee staff to review the responses.

1. The Specter bill makes a number of changes to the existing FISA statute. In reviewing these changes to the statute, it would of course be helpful to know how the FISA court has interpreted it. Please provide copies of any FISA court decisions containing legal interpretations of provisions of FISA that are amended by the Specter bill.

ANSWER: (U) NSA is not in a position to provide these documents because NSA does not control them. In any event, the orders issued by the Foreign Intelligence Surveillance Court are classified documents that are not publicly available. Consistent with long-standing practice, however, the Executive Branch notifies Congress concerning the classified intelligence activities of the United States through appropriate briefings of the respective Intelligence Committees of the Senate and the House of Representatives. Furthermore, in the only case it has ever heard, the Foreign Intelligence Surveillance Court of Review published a redacted version of its decision that did not reveal intelligence sources and methods. *See In re Sealed Case*, 310 F.3d 717 (For. Intel. Surv. Ct. Rev. 2002).

2. At the hearing, General Hayden stated that Section 9 of the Specter bill originated at the NSA. Please explain with regard to each subsection of the Specter bill, including each subsection of Section 9, the degree to which you or anyone at your agency/department had input on it, and to the extent not addressed in the answers to the questions below, whether you support it.

ANSWER: (U) Because of the interactive and cooperative nature of the legislative process, it is not possible to say definitively on which subsections of the bill NSA had substantive input. In response to requests from several Members, NSA provided technical drafting assistance that Congress was free to accept or reject.

3. The Specter bill creates a new Title VII of FISA. Under this title, the FISA court would be granted the authority to issue program warrants. Under the bill, would the government

---

<sup>2</sup> As noted previously, *supra* n.1, the proposed language of S. 2453 (marked JEN06974) continues to be modified. At present, the Senate’s FISA modernization proposal that most closely resembles S. 2453 is S. 3931, the Terrorist Surveillance Act of 2006, as introduced. In most cases, the answers provided herein are responsive to the questions that remain relevant in S. 3931; i.e., where the language in S. 3931 does not substantively change the context of the question. A note has been made to indicate those questions where the significant changes in S. 3931 make the question inapplicable.

ever be required by the statute to seek a warrant from the FISA court to engage in an existing or future electronic surveillance program?

ANSWER: (U) S. 2453 has undergone significant changes that affect this question. Nevertheless, Senator Specter's legislation would not require the Executive Branch to submit an electronic surveillance program to the FISC.

4. Please explain your understanding of the interplay in the new Title VII of FISA created by the Specter bill of the section 701 definitions of "electronic communication," "electronic tracking," and "electronic surveillance program." Also explain how those definitions vary from the definition of "electronic surveillance" in existing FISA Title I.

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

5. In the Specter bill, the newly inserted section 701(6) defines "foreign intelligence information" as having the same meaning as the current statute, but also adds "and includes information necessary to protect against international terrorism." Given the definitions already in the FISA statute, isn't this additional language just duplicative?

ANSWER: (U) NSA continues to evaluate these provisions. Because "foreign intelligence information" is broader and encompasses terrorism, the reference to terrorism merely adds emphasis and does no harm.

6. The current FISA statute defines "contents" as "any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication." The Specter bill, in creating the new Title VII, uses the term "substance" rather than "contents." It defines "substance" as "any information concerning the symbols, sounds, words, purport, or meaning of a communication, and does not include dialing, routing, addressing, or signaling." Please discuss whether you believe this alternate definition is necessary and if so, why. Please also discuss how you believe this alternate definition varies from the new definition of "contents" that Section 9 of the Specter bill would create in the existing FISA Title I.

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

7. In the Specter bill's new section 702, the FISA Court is given jurisdiction to issue an order authorizing an electronic surveillance program "to obtain foreign intelligence information or to protect against international terrorism." The Administration has publicly described the NSA program as involving communications where there is a reasonable basis to believe that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda.
  - a. Do you agree that the bill authorizes program warrants "to obtain foreign intelligence information" even when there is no connection to al Qaeda, and that this is broader even than what the President has stated he has authorized?

ANSWER: (U) Yes. The bill authorizes court orders “to obtain foreign intelligence information” even when there is no connection to al Qaeda. The bill provides flexibility beyond the al Qaeda threat.

- b. Do you agree that the bill authorizes program warrants “to obtain foreign intelligence information” even when there is no connection to terrorism, and that this is broader even than what the President has stated he has authorized?

ANSWER: (U) Yes. The bill authorizes court orders “to obtain foreign intelligence information” as that term is defined in FISA.

8. In the Specter bill’s new section 702, the FISA Court’s initial authorization of an “electronic surveillance program” cannot be for longer than 90 days, but a re-authorization can be for as long as the court determines is “reasonable.” What do you believe is the justification, if any, for not limiting reauthorization to 90 days?

ANSWER: (U) An initial authorization of 90 days would be appropriate in order to enable the Foreign Intelligence Surveillance Court to review the actual initial operation of the program, particularly the functioning of its minimization procedures. Mandating further review every 90 days thereafter, however, would be unnecessary and inefficient, and would undermine the flexibility and agility that is necessary to conduct effective foreign intelligence surveillance. After the FISC has had the opportunity to see a program in operation for a period, it may reasonably conclude that the protections in place are sufficient that reauthorization every 90 days is unnecessary. Rather than impose an artificial limit upon reauthorizations, proposed section 702(a)(2) in S. 3931 would grant to the experienced Article III judges of the FISC the authority to reauthorize an electronic surveillance program for a “reasonable” period of time.

9. The Specter bill’s new section 702(b) establishes guidelines for mandatory transfers of cases to the FISA Court of Review, and refers to “any case before any court.” Do you believe that these mandatory transfer provisions would apply to pending cases?

ANSWER: (U) NSA is not in a position to answer this question. We defer to the answer of the Department of Justice on this question.

10. In the Specter bill’s new section 702(b), the mandatory transfer provision applies to any case “challenging the legality of classified communications intelligence activity relating to a foreign threat, including an electronic surveillance program, or in which the legality of any such activity or program is in issue.” “Electronic surveillance program” is defined in the bill, but there is no definition in the current FISA statute or in the Specter bill of a “classified communications intelligence activity.” What do you read this term to mean, and what types of cases beyond those involving “electronic surveillance programs” do you believe would be covered by this term?

ANSWER: (U) Given the highly classified nature of the intelligence activities of the United States, it would be inappropriate to attempt in this setting to describe specifically those activities

that would fall within the scope of the term “classified communications intelligence activities.” At a minimum, NSA believes the term “classified communications activity” refers to NSA’s activities authorized under Executive Order 12333. The definition of an “electronic surveillance program” in S. 3931 is more limited in scope.

11. In the Specter bill’s new section 702(b), the mandatory transfer provision, cases are transferred to the FISA Court of Review “for further proceedings under this subsection.” But, there is no subsection defining the procedures for the FISA Court of Review’s “further proceedings,” as there was in prior versions of the bill.

- a. Did you or anyone at your agency/department request or suggest that the paragraph in earlier versions of the bill entitled “Procedures for Review” be removed? If so, why?

ANSWER: (U) No.

- b. As you read this subsection, what relief would the FISA Court of Review have the authority to grant if it found that the program at issue were illegal?

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

- c. As you read this subsection, what role would the parties challenging the program play in the FISA Court of Review proceedings?

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

12. The Specter bill’s new section 702(b)(3) preserves “all litigation privileges” for any case transferred to the FISA Court of Review.

- a. Do you read this as being intended to cover the state secret privilege?
- b. If so, has the state secrets privilege ever before been invoked in the FISA court? Why would it be necessary to invoke the state secrets privilege in a court that operates in a one-sided, secret process?

ANSWER: (U) This section has undergone significant changes in S. 3931. These questions are no longer applicable. Furthermore, NSA is not in a position to answer these questions. We defer to the views of the Department of Justice on these questions.

13. The Specter bill repeals sections 111, 309, and 404 of the FISA statute, which, notwithstanding any other law, give the President the authority to use electronic surveillance, physical searches, or pen registers or trap and trace devices without a court order for up to fifteen days following a declaration of war by Congress. Does the Administration support this repeal of these provisions, which on their face appear to grant additional surveillance options to the executive branch in time of war? If so, why?

ANSWER: (U) As explained in the Department of Justice’s *Legal Authorities Supporting the Activities of the National Security Agency Described by the President* (“*Legal Authorities*”) at 6-10 (Jan. 19, 2006), section 111 of FISA (and parallel sections 309 and 404) does not specify the manner in which the President must proceed after the expiration of the 15-day period, nor does it address armed conflicts in which there is no formal declaration of war. We believe, however, that Congress understood that subsequent legislation, including legislation such as the Authorization for Use of Military Force, could authorize electronic surveillance outside traditional FISA procedures. *See Legal Authorities at 2-3, 20* (stating that 50 U.S.C. § 1809(a)(1) contemplates that Congress could authorize electronic surveillance through another statute, such as the AUMF); 50 U.S.C. § 1809(a)(1) (prohibiting any person from intentionally “engage[ing] . . . in electronic surveillance under color of law except as authorized by statute”).

14. The Specter bill, in section 8(c)(2)(A)(i), inserts “or under the Constitution” in 50 U.S.C. § 1809(a)(1). What is the effect of this amendment to section 1809?

ANSWER: (U) This section has undergone significant changes in S. 3931, and this specific question is no longer applicable. Nevertheless, the general purpose of inserting such language is to avoid an unnecessary constitutional conflict regarding whether the FISA unconstitutionally interferes with the authority of the President to conduct electronic surveillance without prior judicial approval for the purpose of collecting foreign intelligence information during an ongoing armed conflict. A statute (such as FISA), of course, cannot eliminate the President’s constitutional authority to conduct surveillance of a foreign enemy without prior judicial approval. *See, e.g., In re Sealed Case*, 310 F.3d 717, 742 (For. Intel. Surv. Ct. Rev. 2002). Accordingly, revising 50 U.S.C. § 1809(a)(1) to make clear that the conduct of foreign intelligence surveillance pursuant to *either* the FISA *or* the Constitution is not unlawful would clarify that FISA should not be construed to infringe on the constitutional authority of the President to conduct surveillance of a foreign enemy during an armed conflict without prior judicial approval.

15. The Specter bill, in section 8(c)(2)(A)(iii), adds a third category of criminal activity to 50 U.S.C. § 1809(a). This third category is similar to the second category, 1809(a)(2).
- Please explain your view of the difference between the language of the new 1809(a)(3), “knowingly discloses or uses information obtained under color of law by electronic surveillance . . .”; and the language of the existing 1809(a)(2), “discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance . . .”
  - Second, the new 1809(a)(3) would add the phrase “in a manner or for a purpose” prior to “authorized.” Do you agree with this added language, and if so, why?
  - Third, it ends with the phrase “authorized by law,” rather than “authorized by statute” as 1809(a)(2) does, or “authorized by statute or under the Constitution,” as the bill would amend 1809(a)(2) to read. Please explain the reason, if any, for not adopting the same phrase as in 1809(a)(2), either in current law or as it would be amended by the bill.

ANSWER: (U) NSA is not in a position to answer this question.

16. The Specter bill, in section 8(c)(2)(B), increases the penalties of violating 50 U.S.C. 1809's criminal prohibitions, both in amount of maximum fines (\$10,000 to \$100,000) and maximum prison term (five years to fifteen years). Do you support these changes? If so, why do you believe they are justified?

ANSWER: (U) NSA is not in a position to answer this question.

17. The Specter bill, in section 9(b)(1), inserts an additional category into the current FISA statute's definition of a non-U.S. person "agent of a foreign power" – someone who "possesses or is expected to transmit or receive foreign intelligence information within the United States." Given that section 1801(b)(1)(C) of FISA already includes any non-U.S. person engaged in "activities in preparation" of international terrorism, do you believe this added language is necessary? If so, why?

ANSWER: (U) Yes, we believe the added language is necessary. This change to FISA is not meant to deal only with terrorism, but with a problem that affects NSA's ability to collect foreign intelligence from non-U.S. persons while they are inside the United States for a limited amount of time. Specific examples could be provided in a classified setting, but the problem may be described in general terms as follows. On numerous occasions, non-U.S. persons come to the United States and either have in their possession or are anticipated to access from within the United States foreign intelligence information that is of vital interest to the United States Government. However, if an individual is not currently an "officer or employee" of a foreign power, or a spy, terrorist or saboteur (or someone who aids or abets someone engaging in espionage, terrorism, or sabotage), the FISC does not have jurisdiction to authorize either physical searches or electronic surveillance directed at that individual. It is important to note that the proposal would not allow intelligence agencies to direct searches or surveillances against visitors to the United States at their discretion. It would merely afford them an opportunity to ask the FISC to authorize the surveillance or search of a non-U.S. person within the United States where a certifying official deems the foreign intelligence information to be significant. Currently, because FISC authorization is not available, intelligence agencies can only seek to obtain the foreign intelligence held or available to such individuals while they are outside the United States. Operating outside the United States puts intelligence gatherers at risk of exposure, imprisonment, or execution.

18. The Specter bill [see footnote 2], in section 9(b)(2), modifies section 1801(f) of FISA, defining "electronic surveillance." The opening language of the definition in 1801(f)(1) – "the acquisition by an electronic, mechanical or other surveillance device" – is replaced with "the installation or use of an electronic, mechanical or other surveillance device." Please explain the effect you think this would have on the FISA process, and any reason you see for the change in definitional language.

ANSWER: (U) The current definitions of "electronic surveillance" in FISA are related to two very different things. The first three definitions apply only to the "acquisition" of communications. The fourth definition is broader, encompassing the installation or use of surveillance devices to acquire not only communications (other than those passed by wire or



radio) but also any other “monitoring to acquire information.” Sometimes, it is only the installation of a surveillance device that may require a court order, while the use does not. For this reason, it was necessary to use “installation or use” from the current fourth definition, rather than “acquisition,” which is used in the first three, if the statute is to govern the full spectrum of surveillance activities directed at persons within the United States.

19. The Specter bill [see footnote 2], in section 9(b)(2), modifies section 1801(f) of FISA, defining “electronic surveillance.” The new section 1801(f)(1) would cover only the “intentional collection of information.” No such limitation exists in the current 1801(f)(1). Please explain what you think would be the effect of this new limitation.

ANSWER: (U) The current definition in section 1801(f)(1) governs only the acquisition of communications through “intentionally targeting that United States person.” The use of “intentional collection of information” is designed to replicate this limitation. The current definition in section 1801(f)(1) does not prohibit the incidental acquisition of communications of a United States person within the United States when someone else (e.g. a non-U.S. person outside the United States) is being targeted. Neither should the new definition.

20. The Specter bill [see footnote 2], in section 9(b)(2), modifies section 1801(f) of FISA, defining “electronic surveillance.” The current language in 1801(f)(1) refers to a person “who is in the United States” while the new language refers to a person “who is reasonably believed to be in the United States.” Please explain what you think would be the effect of this new language.

ANSWER: (U) The proposed change to section 1801(f)(1) would recognize that many of the forms of electronic communication that have come into existence since 1978 are much more portable and present the possibility of targeting someone in an unexpected location. In 1978, NSA reliably could associate a phone number with an area code in a European capital with a telephone physically located in that city. Now, telephone area codes are less reliable indicators of the physical location of their users, with the option to purchase phones with any area code that one desires as well as the growth of roaming agreements that allow portable phones to function around the globe. In addition, even newer services like webmail may be used anywhere in the world that an account user has access to the Internet. In accordance with FISA’s overarching purpose of regulating the collection of foreign intelligence information from United States persons within the borders of the United States, we believe that an order permitting electronic surveillance should be required only where the Government reasonably believes a target is physically in the United States. Under the proposed definition, once an intelligence agency has a reasonable belief that a target has entered the United States, the Government would be obligated to seek authorization for electronic surveillance to continue so long as the target is inside the United States.

21. The Specter bill [see footnote 2], in section 9(b)(2), modifies section 1801(f) of FISA, defining “electronic surveillance.” It would limit the definition in 1801(f)(1) to “the intentional collection of information concerning a particular known person . . . by intentionally targeting that person . . . .” In contrast, the current language of 1801(f)(1) covers the “acquisition . . . of the contents of any . . . communication sent by or intended to



be received by” a particular person who is intentionally targeted. Would this change in the definition mean that if the government targeted an individual to obtain information about someone other than that person, that it would fall outside the definition of “electronic surveillance”? Please explain your view of the effect of this change to the definition.

ANSWER: (U) The first definition of “electronic surveillance” in the current law applies only when the contents of communications are obtained by intentionally targeting someone in the United States. NSA would regard any targeting directed at someone within the United States as constituting intentional targeting of the communications of that person. NSA does not believe that the proposed language would permit it to target someone who was within the United States merely because it could identify an interest in someone else or any other purpose. NSA does not believe that it can nominally “target” foreigners outside the United States without an order from the FISC if the purpose of the collection is to obtain the communications of someone inside the United States with a foreign target.

22. The Specter bill [see footnote 2], in section 9(b)(2), modifies section 1801 of FISA defining “electronic surveillance.” It creates a two-part definition of “electronic surveillance,” in which the second half of the definition covers “any communication” where “both the sender and all intended recipients are in the United States.” In all four parts of the current FISA definition, the phrase “by an electronic, mechanical, or other surveillance device” is used. The second part of the definition in the Specter bill does not use this language. Please explain your view of the legal effect of this omission.

ANSWER: (U) As NSA understands it, the purpose of the definition governing the acquisition of domestic communications was to forestall concerns that because the first definition of surveillance only affected surveillance directed at a particular person within the US, it would allow NSA to target large amounts of domestic communications without targeting any one person and thereby avoid triggering the requirement for an order. NSA does not believe the omission of the phrase “by an electronic, mechanical or other surveillance device” has any negative substantive effect, because it believes that acquisition of domestic communications “under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes” will always be accomplished through the installation or use of some surveillance device. If anything, the absence of this phrase actually acts to broaden the application of the definition, so that acquisition of the information by any means “under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes” would be covered by its terms.

23. The Specter bill [see footnote 2], in section 9(b)(3), modifies section 1801 of FISA defining “Attorney General” to include “a person or persons designated by the Attorney General or Acting Attorney General.” What limit would there be on the ability of the Attorney General to designate individuals, including employees of agencies/departments other than the Justice Department, as “Attorney General” for purposes of FISA? To the degree that your answer references regulations, could the Attorney General amend those regulations without congressional approval?

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

24. The Specter bill [see footnote 2], in section 9(b)(4)(C), modifies the FISA definition of “minimization procedures” by striking 50 U.S.C. § 1801(h)(4), which requires that any contents of communications to which a U.S. person is a party shall not be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a FISA court order is obtained or the Attorney General determines the information indicates a threat of death or serious bodily harm to any person. Please discuss what you believe are the advantages of entirely eliminating 1801(h)(4) from the current FISA statute.

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

25. The current FISA statute, in section 1801(n), defines the covered “contents” of communication as: “when used with respect to a communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.” The Specter bill [see footnote 2], in section 9(b)(5), replaces the definition of “contents” with the definition contained in 18 U.S.C. § 2510(8) – “when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication.”
- a. The new definition does not cover “any information concerning the identity of the parties to such communication.” Please discuss what you believe is the effect of this proposed change.
  - b. The new definition does not cover “any information concerning...the existence...of that communication.” Please discuss what you believe is the effect of this proposed change.

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

26. The Specter bill [see footnote 2], in section 9(c), makes a number of changes to section 1802 of FISA. Section 1802(a)(1) authorizes the President to engage in electronic surveillance without court order for up to one year in certain limited circumstances “under this subchapter.” The Specter bill modifies this phrase to “under this title.” In your opinion, what effect would this change have?

ANSWER: (U) We believe this provision would have no substantive effect.

27. The Specter bill [see footnote 2], in section 9(c), makes a number of changes to section 1802 of FISA. The current section 1802 requires the Attorney General to certify that “the electronic surveillance is solely directed at” the acquisition of certain covered communications. The Specter bill strikes the “solely directed at” phrase. Given this modification, what showing about the surveillance do you believe the Attorney General would have to make to meet the requirements of this provision? Please explain whether you support this change, and if so, why.

ANSWER: (U) NSA supports the change but does not believe it is essential. We note that this provision has been modified significantly in S.3931, in a manner that scales back the provision with which you were concerned.

28. The Specter bill [see footnote 2], in section 9(c), makes a number of changes to section 1802 of FISA, which permits electronic surveillance without a court order in certain limited circumstances. The language of 1802(a)(1)(A)(i) currently requires a showing that the communications being pursued are “communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801(a)(1), (2), or (3) of this title.” The Specter bill, in contrast, would require only that the communications being pursued were “communications of foreign powers, as defined in section 101(a), an agent of a foreign power as defined in section 101(b)(1).” This is a significant expansion of section 1802’s exemption from the usual FISA court order requirement.

- a. Do you support this modified language of section 1802? If so, please discuss the justification for eliminating the limiting language that requires the means of communications be “used exclusively between or among foreign powers.”
- b. If you do support the modified language of section 1802, please explain the justification for expanding the “foreign powers” covered by this blanket exemption from those defined in 1801(a)(1)-(3) to all “foreign powers.”
- c. If you do support the modified language of section 1802, please explain the justification for adding non-U.S. person agents of foreign powers to this blanket exemption.
- d. In combination with the change to the definition of “agent of foreign power” elsewhere in the bill, wouldn’t this mean that the government could wiretap without a warrant the calls of any non-U.S. person in the United States who possessed or was expected to transmit or receive “information with respect to a foreign power or foreign territory that relates to ... the conduct of the foreign affairs of the United States”? Wouldn’t this be a very broad category covering foreign nationals who have nothing to do with terrorism and no intent to harm the United States in any way?

ANSWER: (U) This section has undergone significant changes in S. 3931. As noted above, these changes have scaled back the scope of the proposed provision. This question is no longer applicable.

29. The Specter bill [see footnote 2], in section 9(c), makes a number of changes to section 1802 of FISA, which permits electronic surveillance without a court order in certain limited circumstances. The Specter bill strikes the requirement of 1802 that the Attorney General certify that “there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party.” Please discuss your view of the justification, if any, for repealing this requirement.

ANSWER: (U) The bill would allow the Attorney General to authorize surveillance against these foreign powers as well as non-U.S. persons within the United States without the

requirement that the surveillance be limited to communications exclusively used by such individuals. The intent of these changes is to reflect how intelligence agencies currently handle communications to, from, or about U.S. persons when they are acquired by other means, such as when NSA intercepts communications of U.S. persons in contact with foreign powers overseas. Intelligence agencies acting pursuant to Attorney General certification would handle any U.S. person communications in accordance with approved minimization procedures.

30. The Specter bill [see footnote 2], in section 9(c), makes a number of changes to section 1802 of FISA. In creating a new 1802(b), the Specter bill creates a completely new category of Attorney General authority – that as long as the Attorney General certifies that given information, facilities or technical assistance does not fall within the definition “electronic surveillance,” the Attorney General can require any electronic communications service, landlord, custodian or other person to furnish such information, facilities, or technical assistance. Please discuss what you consider to be the advantages, if any, of this new provision.

ANSWER: (U) The new provision allows the Intelligence Community, through the Attorney General, to obtain the assistance described. In addition, it provides the service providers with the necessary legal protection from liability claims that may result from the assistance they provide pursuant to lawful Government requests.

31. The Specter bill [see footnote 2], in section 9(c), makes a number of changes to section 1802 of FISA. The Specter bill creates a new 1802(c), which is similar to the language of the current FISA section 1802(a)(4) that permits the Attorney General to order carriers to provide assistance to implement section 1802 and allows them to be compensated.
- a. The current 1802(a)(4) only applies to “electronic surveillance authorized by this subsection.” The new 1802(c) would apply to “electronic surveillance or the furnishing of any information, facilities, or technical assistance authorized by this section.” Please discuss your view of the effect of the difference between these two formulations.
  - b. The current 1802(a)(4) also only applies to a “specified communication common carrier.” The new 1802(c) applies to “any electronic communication service, landlord, custodian or other person (including any officer, employee, agent, or other specified person thereof) who has access to electronic communications, either as they are transmitted or while they are stored or equipment that is being or may be used to transmit or store such communications.” Do you agree with this change? If so, please discuss why you believe that this wider scope is needed.

ANSWER: (U) This section has undergone significant changes in S. 3931. Nevertheless, the new formulation is necessary to achieve the goal discussed in the answer to the previous question. The change indicated in part b, or something like it, is necessary to update FISA.

32. The Specter bill [see footnote 2], in section 9(c), creates a new section 1802(d), which reads: “Electronic surveillance directed solely at the collection of international radio communications of diplomatically immune persons in the United States may be authorized by an official authorized by the President to engage in electronic surveillance for foreign

intelligence purposes in accordance with procedures approved by the Attorney General.”  
Please discuss whether you believe this added authorization is necessary, and if so, why.

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

33. The Specter bill [see footnote 2], in section 9(e), would strike requirements (6), (8), (9) and (11) from the section 1804(a) of FISA, the provision that lays out the required components of FISA applications for electronic surveillance.
- a. Please discuss whether you believe these changes are necessary, and if so, why.
  - b. Do you believe that the information required in these paragraphs was not helpful to the FISA court?

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

34. The Specter bill [see footnote 2], in section 9(f)(4), would substantially modify section 1805(e)(1) of FISA, which sets the time limits for a FISA surveillance order. Under current law, FISA surveillance can be authorized for at most ninety days; except that for a non-U.S. person agent of a foreign power, it can be 120 days at most; and for surveillance of certain types of foreign powers, a year at most. The Specter bill replaces these three tiers with a single time limit – a maximum limit of a court order of surveillance for one year – even for U.S. persons.
- a. Please discuss whether you believe this change is necessary, and if so, why.
  - b. Please explain your understanding of what is intended by the second sentence of the new 1805(e)(1) that would be created by the Specter bill: “If such emergency employment of electronic surveillance is authorized, the official authorizing the emergency employment of electronic surveillance shall require that the minimization procedures required by this title for the issuance of a judicial order be followed.”

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

35. The Specter bill [see footnote 2], in section 9(g), modifies section 1806(i) of FISA, which requires the destruction of certain communications contents that were unintentionally acquired unless the Attorney General determines they indicate a threat of death or serious bodily harm to any person. The amendment would allow the Attorney General to retain any unintentionally acquired communications contents that he determines contains “significant foreign intelligence.”
- a. Please discuss whether you believe this change is necessary, and if so, why.
  - b. In making this determination, what procedures do you believe the law would require the Attorney General to undertake?

ANSWER: (U) This section would only apply to the inadvertent interception of domestic communications transmitted by any means (not just radio communications, if the statute

becomes “technology neutral”). We believe this change is necessary because the current standard is extraordinarily high and could require the destruction of extremely valuable intelligence. As an example, in the course of collecting international communications, NSA might inadvertently intercept a domestic communication in which it is revealed that a spy for a foreign nation has slipped into the United States undetected. Under such circumstances, the statute may require destruction of the information unless the Attorney General determines that this information indicated a “threat of death or serious bodily harm to any person.” Requiring that the Attorney General make a specific determination that the information was “significant foreign intelligence” is a reasonable alternative.

36. The Specter bill, in section 9(i), strikes section 1809(a) of the current FISA and replaces it with new language. But the Specter bill, in section 8(c), makes different line-by-line amendments to section 1809(a) of the FISA statute. Do you agree that these two provisions of the proposed legislation are inconsistent and cannot both become law? Of the two provisions, which do you support and why?

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

37. The Specter bill, in section 9(k), modifies section 1827 of FISA by expanding the exception to the criminal prohibition of warrantless physical searches in section 1827(a)(1) to include “except as authorized...under the Constitution.” What authority to do warrantless physical searches do you believe is granted “under the Constitution”? Also please discuss whether you believe this change is necessary, and if so, why.

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.

38. The Specter bill, in section 9(k), modifies section 1827(a)(2) of FISA by omitting the phrase – “for the purpose of obtaining intelligence information.” Please discuss whether you believe this change is necessary, and if so, why.

ANSWER: (U) This section has undergone significant changes in S. 3931. This question is no longer applicable.