OFFICE of the Director of National Intelligence
Washington, DC 20511

September 17, 2007

The Honorable Silvestre Reyes
Chairman
Permanent Select Committee
on Intelligence
House of Representatives
Washington, DC 20515

The Honorable Peter Hoekstra
Ranking Member
Permanent Select Committee
on Intelligence
House of Representatives
Washington, DC 20515

Dear Mr. Chairman and Representative Hoekstra:

I am writing this letter in response to a request from the Ranking Member of the House Permanent Select Committee on Intelligence. I appreciate this opportunity to describe the civil liberties and privacy protections that my office is charged with overseeing in the implementation of the Protect America Act of 2007.

Role of the Civil Liberties Protection Officer. I am the Civil Liberties Protection Officer for the Office of the Director of National Intelligence (ODNI). Congress has entrusted me with statutory responsibility to "ensure that the protection of civil liberties and privacy is appropriately incorporated in the policies and procedures" of the Intelligence Community. 50 U.S.C. § 403-3d(b)(1). As a result, my office is working closely with the Department of Justice and the DNI's Office of General Counsel, to help ensure that the intelligence agencies that implement the authorities under the Protect America Act have put in place adequate safeguards to protect the privacy and civil liberties of American citizens, legal residents, organizations and corporations ("U.S. persons"), as required by law and by the rules that have traditionally governed our intelligence activities. In addition, my office is working with the Department of Justice and DNI's Office of General Counsel to conduct formal, periodic assessments of compliance by agencies exercising authorities under the Protect America Act, and briefing the staffs of various congressional committees frequently and in depth.

The Larger Context - Protection of Civil Liberties and Privacy in the Intelligence Community. In order to understand the civil liberties and privacy protections that are being implemented under the Protect America Act, it is important to put the Act in the larger context of

how the Intelligence Community has historically protected information about Americans. As you know, intelligence agencies collect, retain, and disseminate information about U.S. persons. One of the limitations placed on the collection and use of U.S. person information is found in Executive Order 12333. That Executive Order provides that collection of intelligence is to be "pursued in a vigorous, innovative and responsible manner that is consistent with the Constitution and applicable law and respectful of the principles upon which the Constitution was founded." It was signed by President Reagan in 1981, building on similar orders signed by Presidents Ford and Carter, to address the findings of the Church and Pike committee investigations of the mid-1970s. It put in place key restrictions on intelligence activities, sometimes referred to as "U.S. person rules," and has become part of the fabric of the Intelligence Community.

These rules – further detailed by procedures approved by the Attorney General for each agency – are not implemented in a vacuum. They are interpreted and applied by offices of general counsel at each intelligence agency, with compliance audited by offices of inspector general.[1] And of course, as you and the members of your committee are well aware, a critical outcome of the Church and Pike reports was the establishment of the House and Senate Intelligence Committees. Since the nature of intelligence by necessity requires secrecy, and therefore full transparency cannot be provided to the public at large, the Intelligence Committees, by exercising oversight over classified activities, can ensure that the Intelligence Community is protecting the nation from foreign threats while at the same time protecting our civil liberties.[2]

The Protect America Act. As Director McConnell and others have explained, as a result of technology changes in the global communications network, in recent years a substantial volume of communications of persons in foreign countries have been subject to the Foreign Intelligence Surveillance Act (FISA) despite Congress's intent in 1978 to exclude such activities. These changes resulted in applying the framework of probable cause and prior court review to foreign intelligence targets in foreign countries. In passing the Protect America Act, Congress changed the law to exempt from electronic surveillance "surveillance directed at a person reasonably believed to be located outside the United States" in order to obtain "significant foreign intelligence." As a result, probable cause and prior court review are not required for surveillance of foreign intelligence targets in foreign countries for foreign intelligence purposes.

Congress was concerned, however, with (1) whether the target of the surveillance is really in a foreign country, and (2) the privacy and civil liberties interests of U.S. persons who may be in communication with the target. To address these two issues, Congress required the Director of National Intelligence and the Attorney General to certify two separate sets of procedures with respect to acquisitions conducted under the Protect America Act:

---

[1] Violations of these rules are required to be reported to the Intelligence Oversight Board of the President's Foreign Intelligence Advisory Board. See Executive Order 12334 (Dec. 4, 1981) (establishment of Intelligence Oversight Board).

[2] Moreover, violations of law are required to be reported to the Intelligence Committees. See National Security Act of 1947, as amended, 50 U.S.C. § 413(b).

(1) reasonable procedures for determining that surveillance to be conducted pursuant to the Protect America Act concerns persons reasonably believed to be outside the United States ("foreign targeting procedures"), which must be reviewed by the FISA court, and

(2) minimization procedures that meet the definition of "minimization procedures" under FISA.[3]

In conjunction with the Department of Justice and the DNI's Office of General Counsel, we are focusing our oversight on ensuring that both sets of procedures adequately protect the privacy and civil liberties of U.S. persons, and that they are being followed by agencies of the Intelligence Community.

Is the target really a foreign intelligence target in a foreign country?

My office, the Department of Justice, and the DNI's Office of General Counsel has reviewed the foreign targeting procedures to ensure that they protect privacy and civil liberties, and is involved in reviewing their implementation to ensure that the procedures are followed. The statute does not require perfection, but it does require procedures that ensure collection is only undertaken against persons "reasonably believed to be outside the United States."

The need to perform this analysis is nothing new for the National Security Agency or other Intelligence Community agencies. Agencies have developed, over decades, policies and procedures to ensure that their monitoring activities did not inadvertently collect domestic information by mistake. However, in the Protect America Act, Congress went a step further, by requiring these procedures to be certified by the Director of National Intelligence and the Attorney General and submitted for review by the Foreign Intelligence Surveillance Court.

Significantly, the statute applies the foreign targeting procedures to "the acquisition of foreign intelligence information . . . ." As a result, the Intelligence Community's procedures for this kind of collection must enable analysts to determine, prior to obtaining any communications under the Protect America Act, that there is a reasonable belief that the target is a foreign intelligence target in a foreign country. Detailed procedures, which have already been submitted to the Foreign Intelligence Surveillance Court, explain how this is done. The procedures are classified because they discuss precisely how the Intelligence Community performs collections. However, I can describe them in general terms.

This "foreign targeting" determination that analysts must make may be relatively straightforward for certain forms of communication, and may be more complex for other forms of communication. The Intelligence Community uses a variety of sources of information, including technical analysis, information about the target from other intelligence reporting, and databases that are commercially available or otherwise lawfully obtained. Analysts are generally

[3] Section 105B of FISA, as amended by the Protect America Act, requires the Director of National Intelligence and the Attorney General to certify, among other things, that: "there are reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be outside the United States, and such procedures will be subject to review of the [FISA] Court . . ." and that "the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under [FISA]."

able to assess, with a high degree of confidence, whether a particular foreign intelligence target is in a foreign country. When they cannot do so, they will not initiate collection against that target.

While the procedures require this foreign targeting determination to be made prior to initiating collection, a variety of means are also employed to verify that the determination continues to be accurate after collection has begun. Even where the initial decision was correct, the location of the target may change. The Intelligence Community does not simply rest on its initial decision. Methods used to double-check the foreign targeting determination are employed frequently, even daily in some cases.

Questions have been raised about Americans traveling or residing abroad. Section 2.5 of Executive Order 12333 protects Americans – and U.S. persons generally – who may be encountered by the Intelligence Community overseas, by prohibiting the use of techniques that would require a warrant if used for law enforcement purposes, unless the Attorney General has determined that there is probable cause to believe the U.S. person is an agent of a foreign power. This requirement – in place since 1981 – has been judicially reviewed and upheld,[4] and is not affected by the Protect America Act. As a result, analysts must – and do – take steps to ensure that their "foreignness" determinations under the Protect America Act not only involve an assessment of the target's location, but also of whether the target may be a U.S. person. If the target is a U.S. person, collection may not be initiated without authorization under section 2.5 of Executive Order 12333, based on a finding of probable cause that the target is an agent of a foreign power.[5]

Questions have also been raised about "reverse targeting" – that is, could an intelligence agency target a person overseas as a pretext for intercepting the communications of the individuals inside the United States with whom the foreign person is in contact? The simple answer is that when the agency's actual purpose is to surveil the person in the United States, it must obtain a court order as required under FISA. This is also not a new problem for either the intelligence or law enforcement communities. When wiretapping the phone of any target – be it the NSA targeting a foreign terrorist or the FBI obtaining a law enforcement warrant to tap the phone of an organized crime figure – it is inevitable that conversations will be overheard with "incidental interceptees," individuals who are not the original targets but who might disclose information of interest.

The concerns about how to police this in practice are understandable, yet it is difficult to come up with a strict quantitative or other bright line test on such matters. You should rest assured that I intend to work closely with the Department of Justice, the DNI's Office of General Counsel, and the offices of general counsel of the agencies involved to develop further training and guidance in this area as needed, to safeguard against reverse targeting and protect privacy and civil liberties. It is important to recognize, also, that reverse targeting makes little sense as a

---

[4] In *United States v. Bin Laden*, 126 F. Supp. 2d 264, 277 (S.D.N.Y. 2000), the court "adopt[ed] the foreign intelligence exception to the warrant requirement for searches targeting foreign powers (or their agents) which are conducted abroad." See also *United States v. Duggan*, 743 F.2d 59, 71 (2d Cir. 1984) (citing cases); *United States v. Marzook*, 435 F. Supp. 2d 778 (E.D. Ill. 2006) (upholding 1993 physical search under section 2.5).

[5] The court in *United States v. Bin Laden*, 126 F. Supp. at 282 n.23, also noted that it did "not take issue with the policies and procedures" of section 2.5.

matter of intelligence tradecraft: if intelligence officers are indeed interested in a target inside the United States, they will have a natural incentive to seek a FISA court order in any event so as to obtain all of that person's communications, rather than the limited subset that would otherwise be acquired through such reverse targeting.

Are minimization procedures protecting the privacy and civil liberties of U.S. persons?

As discussed above, when the communications of persons overseas are acquired, it is inevitable that some of those communications will incidentally involve U.S. persons. Again, this is a familiar challenge for the Intelligence Community. In general, "minimization procedures" are procedures for reviewing, handling, and, as appropriate, destroying, information about U.S. persons, depending on whether or not the information constitutes foreign intelligence information or fits within another category the agency is authorized to retain. The FISA statute fully embraces and incorporates the concept of minimization as a way of dealing with the inevitability of incidentally intercepting communications of U.S. persons during authorized FISA surveillance.[6]

The Protect America Act requires that similar minimization procedures be followed with respect to surveillance conducted under the Act. These minimization procedures are intended to protect the privacy and civil liberties of U.S. persons who may be communicating with targets overseas. The Act requires that these procedures meet the definition of "minimization procedures" under FISA. My office, the Department of Justice, and the DNI's Office of General Counsel, have reviewed the minimization procedures, and, as part of our periodic compliance assessments, are reviewing compliance with those procedures. These procedures have been made available to the Intelligence Committees. Although not required by the Protect America Act, it should be noted that NSA is using minimization procedures previously reviewed and approved by the Foreign Intelligence Surveillance Court.

Because the minimization procedures used for the Protect America Act are themselves classified, it may be helpful in this unclassified letter to review those procedures for collecting, retaining, and disseminating U.S. person information in place at NSA, that have been released in

[6] FISA defines "minimization procedures" as:

(1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information; (2) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in subsection (e)(1), shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and (4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 102(a), procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 105 is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

unclassified form. While these minimization procedures are not identical to the ones used for the Protect America Act, they provide general guidance for the types of processes and requirements involved with minimization.

United States Signals Intelligence Directive 18 (USSID 18) implements the requirements of Executive Order 12333 for the signals intelligence system. USSID 18 states plainly that "The Fourth Amendment to the United States Constitution protects all U.S. persons anywhere in the world and all persons within the United States from unreasonable searches and seizures by any person or agency acting on behalf of the U.S. government." (§ 1.1). While some portions of the USSID are classified because they reveal sensitive sources and methods, most of it is unclassified and it has been periodically released under the Freedom of Information Act.[7] USSID 18 applies specific rules for retention, processing, and dissemination of any for communications that are to, from or about U.S. persons:

- Such communications may generally only be retained in raw form for a maximum of five years, unless there is a written finding that retention for a longer period is necessary to respond to a foreign intelligence requirement (§ 6.1.a(1));

- Intelligence reports from such communications are written "so as to focus solely on the activities of foreign entities and persons and their agents." (§ 7.1)

- Identities of U.S. persons are generally redacted from intelligence reports and replaced with generic terms such as "U.S. person" or "U.S. firm." Deleted identities are retained for a maximum of one year. (§ 7.1)

- U.S. person identities may generally be released only where the U.S. person has consented to such release, the information about the U.S. person is publicly available (e.g., a foreign target discussing a news report), or the identity of the U.S. person is necessary to understand foreign intelligence information or assess its importance (§ 7.2).

- The USSID lists specific responsibilities, including regular inspections, reports, legal reviews, and training for the Inspector General, General Counsel, and Deputy Director for Operations. Violations must be reported on a quarterly basis to the President's Foreign Intelligence Advisory Board through the Assistant to the Secretary of Defense for Intelligence Oversight. (§ 8).

USSID 18 also contains standard minimization procedures for surveillance conducted by NSA pursuant to the Foreign Intelligence Surveillance Act. These procedures supplement the standard USSID 18 procedures for all signals intelligence activities. They apply substantially the same process, with a few additional safeguards, notably that:

- The acquisition must be made in a manner "designed to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the surveillance." (App. 1, § 3(a)).

[7] A redacted version is available from the National Security Archive, a non-profit organization affiliated with George Washington University, at http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/07-01.htm

- The lines or numbers being targeted must be verified as the lines or numbers authorized, and collection personnel must, at regular intervals, confirm "that the surveillance is not avoidably acquiring communications outside the authorized scope of the surveillance." (App. 1, § 3(b)).

In sum, the Protect America Act puts in place privacy and civil liberties protections (1) to help ensure the targets of surveillance are located outside the United States, and (2) to minimize information that is not necessary to understand foreign intelligence or assess its importance in communications to, from or about U.S. persons.

Other Questions

Questions have also been raised about other potential uses – and mis-uses –of authorities granted under the Protect America Act. On September 14, Assistant Attorney General Kenneth Wainstein explained why the Protect America Act does not authorize – among other things – reverse targeting, surveillance of domestic communications that merely "concern" a foreign target, physical searches of Americans' homes, effects or mail, or obtaining Americans' medical or library records. The oversight mechanisms outlined below will help ensure that the Protect America Act is being applied in a manner consistent with those interpretations.

Questions might also be raised as to whether the Protect America Act could enable the Intelligence Community to conduct surveillance for non-intelligence purposes. The requirement that surveillance under the Protect America Act be for "foreign intelligence" purposes also would prohibit abusing such authority for surveillance of Americans' political, religious, or any other domestic activities. Moreover, the provisions of Executive Order 12333 and each agency's Attorney General-approved procedures have for decades required that agencies demonstrate a valid mission-related purpose for collecting, retaining, or disseminating information about a U.S. person.

Other Offices and Institutions Involved in Oversight

While my office takes its oversight responsibilities very seriously, as discussed throughout this letter, it is not alone. As described in more detail in the September 5, 2007 letter of Principal Deputy Assistant Attorney General Brian Benczkowski, the Department of Justice, through the National Security Division, and the Director of National Intelligence, through my office and the DNI's Office of General Counsel, are conducting reviews of the implementation of the Protect America Act. These reviews started within 14 days of the initiation of collection under the Protect America Act and every 30 days thereafter. I am conducting these reviews together with the ODNI's Office of General Counsel and the National Security Division of the Department of Justice.

The following other offices and institutions, in all three branches of government, have a direct role in oversight of the Protect America Act – this list is not exhaustive:

Executive Branch, within the Intelligence Community:

- The Inspector General of the NSA conducts regular audits, inspections and reviews of compliance with USSID 18 and minimization procedures – it is also conducting an audit of the implementation of the Protect America Act;

- The General Counsel of the NSA provides legal advice and assistance and performs oversight in accordance with USSID 18 and the Protect America Act. It also helped develop the training courses on USSID 18 and the Protect America Act and supports administration of the training to the NSA workforce;

- The Signals Intelligence Directorate Oversight and Compliance Office provide oversight and compliance for the implementation of the Protect America Act at NSA;

- Other agency offices of general counsel and offices of inspector general perform similar oversight roles with respect to their agencies' use of this authority;

- The Office of General Counsel of the ODNI provides legal advice and assistance to the DNI in making his certifications under the Act, in assessing compliance with the procedures, an in reporting those assessments to Congress.

Executive Branch, outside the Intelligence Community:

- The Justice Department's National Security Division is conducting compliance assessments, as it does with respect to other FISA authorized activities;

- The Justice Department's National Security Division, the Office of Legal Policy and the Office of Legal Counsel are providing policy and legal advice with respect to the Protect America Act;

- The Justice Department's Civil Liberties and Privacy Office is consulting with the National Security Division in its assessments under the Protect America Act;

- The Privacy and Civil Liberties Oversight Board, currently within the Executive Office of the President, is conducting its own review of the policies and procedures of the Protect America Act;

- The Assistant Secretary of Defense for Intelligence Oversight reviews reports of violations by NSA, and other Defense Department intelligence entities, on a quarterly basis;

- The Intelligence Oversight Board of the President's Foreign Intelligence Advisory Board receives reports of violations on a quarterly basis;

- The DoD Office of Inspector General also conducts regular audits, inspections and reviews of compliance with USSID 18 and minimization procedures.

Legislative Branch

- The Permanent Select Committee on Intelligence of the House of Representatives, and the Select Committee on Intelligence of the Senate are conducting intensive oversight of the Protect America Act.

- Members and staff have engaged in multiple oversight visits at the NSA;

- Both committees have held open and closed hearings on the subject, and have received numerous staff and member briefings.

- The House and Senate Judiciary Committees have likewise received oversight briefings, have conducted oversight visits, and have held public hearings.

- Congress will have an opportunity to revisit and clarify language in the Protect America Act before extending the Act or making it permanent.

Judicial Branch

- The Foreign Intelligence Surveillance Court has a direct role under the statute in reviewing procedures by which the Intelligence Community determine that a target is outside the United States.

- These procedures have already been submitted to the court and are currently under review.

- A recipient of a directive under section 105B of the Protect America Act may challenge its legality before the Foreign Intelligence Surveillance Court.

This extensive oversight helps ensure that agencies implementing the authorities of the Protect America Act are doing so in a careful, thoughtful, way that is fully transparent to the Congress, and that demonstrates due regard for the protection of privacy and civil liberties of Americans.

I hope this information is helpful. If you have any questions or would like more information on any of these issues, please contact Kathleen Turner in the Office of Legislative Affairs at (202) 201-1698.

Sincerely,

Alexander W. Joel