FAS Note: The following Report was required by the FY 2000 Intelligence Authorization Act, and was transmitted to Congress at the end of February 2000.

Legal Standards for the Intelligence Community in Conducting Electronic Surveillance

(U) Electronic surveillance is conducted by elements of the Intelligence Community for foreign intelligence and foreign counterintelligence purposes. Because of its potential intrusiveness and the implications for the privacy of United States persons,[1] such surveillance is subject to strict regulation by statute[2] and Executive Order[3] and close scrutiny. The applicable legal standards for the collection, retention, or dissemination of information concerning U.S. persons reflect a careful balancing between the needs of the government for such intelligence and the protection of the rights of U.S. persons, consistent with the reasonableness standard of the Fourth Amendment,[4] as determined by factual circumstance.

[1] "United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an associated which is a foreign power, as defined in 50 U.S.C. §1801(a)(1), (2), or (3). See 50 U.S.C. §1801(i).

[2] The Foreign Intelligence Surveillance Act, 50 U.S.C. §1801 et seq.

[3] Exec. Order No. 12333, 3 C.F.R. 200 (1982), reprinted in 50 U.S.C. §401 note.

[4] The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. U.S. Const. Amend. IV.

(U) In the Foreign Intelligence Surveillance Act (FISA) and Executive Order (E.O.) 12333, Congress and the Executive have codified this balancing. Both documents reflect a deference to U.S. persons' rights by closely regulating the conduct of electronic surveillance that either targets U.S. persons or may result in the acquisition of information to, from, or about U.S. persons. For example, 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. If the United States person is abroad, the Executive Order

requires that the Attorney General approve such surveillance. In both instances, generally speaking there must be probable cause [5] that the target is an agent of a foreign power. [6] In addition, the information sought by the surveillance must be foreign intelligence that cannot be obtained by other less intrusive collection techniques. Furthermore, even if a U.S. person is not the target, all foreign intelligence electronic surveillance must be conducted in a manner that minimizes the acquisition, retention, and dissemination of information about unconsenting U.S. persons.[7] Information about a U.S. person who is not an approved target, if lawfully acquired incidental to the authorized collection, may be retained and disseminated if it amounts to foreign intelligence or counterintelligence; otherwise, it may not be retained or disseminated.

[5] Probable cause exists when facts and circumstances within the applicant's knowledge and of which he/she has reasonably trustworthy information are sufficient to warrant a person of reasonable caution to believe that the proposed target of the surveillance is an agent of a foreign power. See generally, United States v. Cavanagh, 807 F.2d 787 (9th Cir. 1987).

[6] Pursuant to §2.3 of E.O. 12333, there may be other instances where U.S. person information may be collected, such as with the consent of the person concerned or where the information is needed to protect the safety of any persons or organizations, including those who are targets, victims, or hostages of international terrorist organizations.

[7] Pursuant to §2.3 of E.O. 12333, Intelligence Community agencies are authorized to retain and disseminate incidentally acquired information that may indicate involvement in activities that may violate federal, state, local, or foreign laws.

(U) As alluded to above, FISA is the statutory regime governing electronic surveillance within the United States for foreign intelligence purposes. Enacted in 1978, FISA defines four types of electronic surveillance requiring Court authorization. The Act further mandates the filing of an application approved by the Attorney General setting forth probable cause that the target of the proposed electronic surveillance is either a foreign power or an agent of a foreign power as defined by the statute. The purpose must be to gather foreign intelligence information, and a certification to that effect by a senior Executive Branch official must accompany every application. If a U.S. person, acting as an agent of a foreign power, is the target of the proposed surveillance, the government must satisfy a more stringent standard than that which pertains when the target is not a U.S. person. It is sufficient in the case of a non-U.S. person to show that the information to be acquired is merely *related* to the national defense or security of the United States of the conduct of foreign affairs; where a U.S. person is involved, the contents of the application must include a showing that the acquisition of such information is *necessary* to national defense or security or the conduct of foreign affairs.

(U) In addition, FISA requires the government generally to minimize the amount of information acquired or retained and prohibits, with limited exception, the dissemination of nonpublic information about nonconsenting U.S. persons, consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.[8] The Attorney General, as required by statute, has adopted and filed with the Court specific procedures designed to effectuate the statutory minimization procedures. These procedures are also reported to the intelligence committees of Congress. Among other things, the procedures ensure that the surveillance technique employed minimizes the likelihood of acquiring information, and the amount of information acquired, concerning U.S. persons. The procedures also limit the retention of incidentally acquired information concerning U.S. persons. Finally, the procedures restrict the dissemination of U.S. person-identifying information to the statutorily prescribed bases.

[8] 50 U.S.C. §1801(h)

(U) While FISA provides the statutory basis for conducting electronic surveillance within the

United States for foreign intelligence purposes, E.O. 12333 establishes the overall framework for the conduct of intelligence activities by U.S. intelligence agencies, including the use of electronic surveillance. The Order, which was issued by President Reagan in 1981, governs the conduct of intelligence activities applicable to all intelligence agencies, and also identifies specific responsibilities for each of the agencies.

(U) The overall scheme of the Order is premised upon the determination that the "[c]ollection of [foreign intelligence information] is a priority objective and will 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 United States was founded." 9 Primary among these principles is the need to respect the rights of U.S. persons. The Order mandates that intelligence agencies "shall use the least intrusive collection techniques feasible within the United States or directed against U.S. persons abroad."[10] It proscribes the acquisition of information concerning the domestic activities of U.S. persons.[11] And, it forbids intelligence agencies from requesting other parties to undertake activities that are forbidden in the Order.[12]

[9] E.O. 12333 §2.1.

[10] E.O. 12333 §2.4.

[11] E.O. 12333 §2.3(b).

[12] E.O. 12333 §2.12.

(U) E.O. 12333 prohibits the collection, retention, or dissemination of information about U.S. persons except pursuant to procedures established by the head of the agency and approved by the Attorney General. Each of the intelligence agencies has promulgated such procedures. (See the appendices in the classified version of this report.) The CIA procedures are embodied in Headquarters Regulation (H.R.) 7-1 entitled, "Law and Policy Governing the Conduct of Intelligence Activities." NSA is governed by Department of Defense Directive 5240.1-R, "DoD Activities that May Affect U.S. Persons," including a classified appendix particularized for NSA. The guidelines are further enunciated within NSA through an internal directive, U.S. Signals Intelligence Directive 18. The FBI procedures are contained in "Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations." Any changes to the procedures implemented pursuant to the Order require Attorney General approval, and such changes are also brought to the attention of the congressional intelligence committees as well as the Intelligence Oversight Board of the President's Foreign Intelligence Advisory Board. Each agency's procedures contains specific provisions that address the conduct of electronic surveillance, to include the acquisition, retention, and dissemination of information to, from, or concerning United States persons.

Legal Standards

A. The Legal Standards for Interception of Communications When Such Interception May Result in the Acquisition of Information from a Communication to or from United States Persons.

(U) The legal standards are reflected in the Attorney General minimization procedures mandated by FISA and in the Attorney General-approved procedures mandated by E.O. 12333. The procedures are designed to ensure that electronic surveillance is conducted in a reasonable manner such that a minimum amount of information about U.S. persons who are not authorized targets will be acquired. 13 The procedures are designed to ensure that electronic surveillance is conducted in a reasonable manner. Information about a U.S. person who is not an approved target, if lawfully acquired incidental to the authorized collection, may be retained and disseminated if it amounts to foreign intelligence or counterintelligence; otherwise, it may not be

retained or disseminated.

[13] DoDD 5240.1-R, Classified Annex §4.A.3; USSID 18 §5 and Annex A; FBI FISA Minimization Procedures §3.

B. The Legal Standards for Intentional Targeting of the Communications to or from United States Persons.

(U) The legal standards governing the targeting of U.S. persons in the United States are set forth in FISA and in Attorney General minimization procedures mandated by FISA. With respect to U.S. persons outside the United States, section 2.5 of E.O. 12333 establishes the standards, and the Attorney General-approved procedures required under E.O. 12333 [14] provide the implementing guidelines. The requirements in both instances include a finding, by a Foreign Intelligence Surveillance Court judge in the former case and the Attorney General in the latter instance, that on the basis of the facts submitted there is probable cause to support a finding that an individual is an agent of a foreign power.

[14] H.R. 7-1, Annex A(V)(D); DoDD 5240.1-R, Classified Annex §4.A.1(a)(4); Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations.

C. The Legal Standards for Receipt from Non-United States Sources of Information Pertaining to Communication to or from United States Persons.

(U) Receipt of U.S. person information from non-United States sources is governed by section 2.12 of E.O. 12333, which precludes an agency of the Intelligence Community from participating in or requesting any person to undertake activities forbidden by the Order. As discussed above, the Intelligence Community is not permitted to target U.S. persons absent specific authorization. Agencies in the Intelligence Community similarly are prohibited by section 2.12 of E.O. 12333 from having other parties engage in activities to circumvent these authorization requirements on their behalf. The Intelligence Community, having secured Attorney General approval to engage in electronic surveillance against a U.S. person abroad, may request that a foreign government conduct the collection. The Intelligence Community may also accept incidentally acquired information about U.S. persons from foreign governments. In both cases, the retention and dissemination of U.S. person information from non-U.S. sources is treated in accordance with E.O. 12333 and the Attorney General-approved implementing procedures.[15]

[15] For NSA, DoDD 5240.1-R, Procedure 2 defines collection to include receipt or acceptance by an intelligence community employee of information from a foreign government. Thus all of the restrictions contained in Procedure 2 regarding Collection, Procedure 3 regarding Retention, Procedure 4 regarding Dissemination and Procedure 5 regarding Electronic Surveillance are applicable to the receipt from non-U.S. sources of information pertaining to the communications of U.S. persons.

D. The Legal Standards for Dissemination of Information Acquired Through the Interception of the Communications to or from United States Persons.

(U) The dissemination of information about U.S. persons that was obtained through electronic surveillance authorized by FISA is governed by the statute and the Attorney General-adopted minimization procedures mandated by the statute. Information about U.S. persons that was obtained pursuant to the provisions of E.O. 12333, including incidentally acquired information, may be disseminated only in accordance with Attorney General-approved procedures. [16] The overarching standard as implemented in both E.O. 12333 and FISA minimization procedures [17] is that to disseminate personally identifiable information concerning a U.S. person, the information must be found necessary to understand a particular piece of foreign intelligence or assess its importance.

[16] See §2.3 of E.O. 12333 for other instances where dissemination of this information is permitted.

[17] H.R. 7-1, Appendix D; NSA's FISA Minimization Procedures §6; DoDD 5240.1-R, Classified Annex §4.A.4; USSID 18 §7; Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations; FBI FISA Minimization Procedures §5.

Appendices
(To accompany classified report only)

Appendix A: CIA Headquarters Regulation 7-1, "Law and Policy Governing the Conduct of Intelligence Activities."

Appendix B: DoD Directive 5240.1-R, "DoD Activities that May Affect U.S. Persons," including Classified Annex (Attorney General Procedures for NSA).

Appendix C: U.S. Signals Intelligence Directive 18.

Appendix D: Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations.

Appendix E: FBI's FISA Minimization Procedures.