



Homeland Security

March 27, 2006

MEMORANDUM FOR: All Employees, Detailees, and Contractors Supporting the Office of Intelligence and Analysis

FROM: *MZC*
Associate General Counsel (I&A)

SUBJECT: Intelligence Oversight Basics¹

Introduction, Authorities, and Overview

The Department of Homeland Security's (DHS) Office of Intelligence and Analysis (I&A) is a member of the United States Intelligence Community². As such, I&A is subject to Executive Order 12333, "United States Intelligence Activities," which establishes the basic tenets of Intelligence Oversight. The purpose of the Intelligence Oversight process is to enable I&A intelligence professionals to effectively carry out their authorized functions, while ensuring that their activities affecting U.S. persons are conducted in a manner that protects the constitutional rights and privacy of those U.S. persons.

Upon approval of the Attorney General, Management Directive 8202, "Procedures Governing Activities of the Office of Intelligence and Analysis that Affect United States Persons," implements Executive Order 12333 for I&A. The guidance contained in this document is designed to serve as a handy reference tool for all I&A personnel involved in intelligence activities. The guidance contained herein, however, does not substitute for legal review of specific intelligence activities and any questions on the applicability or interpretation of this guidance should be directed to the DHS OGC (I&A) legal staff.

In order to understand Intelligence Oversight, you must be familiar with the following core concepts: (1) I&A's mission, and (2) the collection, (3) retention, and (4) dissemination of information about United States (U.S.) persons³. Each of these core concepts is explained below.

¹ This memorandum revokes the memorandum, "Intelligence Oversight Basics for the Office of Information Analysis," dated November 1, 2004.

² <http://www.intelligence.gov>; See also, § 201(h) of the Homeland Security Act of 2002, the National Security Act of 1947, and Executive Order 12333 as amended by Executive Order 13284.

³ For purposes of Intelligence Oversight, the definition of a United States (U.S.) person includes: (a) a U.S. citizen; (b) an alien known by IA to be a permanent resident alien; an unincorporated association substantially composed of (a) or (b); (c) a corporation incorporated in the U.S., except for a corporation directed and controlled by a foreign government(s). A corporation or corporate subsidiary incorporated abroad, even if partially or wholly owned by a corporation incorporated in the U.S., is not a U.S. person. A person or organization outside the U.S. shall be presumed not to be a U.S. person unless specific information to the contrary is obtained. A person or organization within the U.S. shall be presumed to be a U.S. person unless specific information to the contrary is obtained. However, an alien within the U.S. shall be presumed not to be a U.S. person unless IA obtains specific information to the contrary.

IA's Intelligence Mission

The primary responsibilities that comprise I&A's intelligence mission, pursuant to Section 201(d) of the Homeland Security Act of 2002, are as follows:

- Access, receive, and analyze law enforcement information, intelligence information, and other information from agencies of the federal government, state and local government agencies (including law enforcement agencies), and private sector entities, and integrate such information in order to: (a) identify and assess the nature and scope of terrorist threats to the homeland; (b) detect and identify threats of terrorism against the United States; and (c) understand such threats in light of actual and potential vulnerabilities of the homeland.
- Integrate relevant information, analyses, and vulnerability assessments in order to identify priorities for protective and support measures by DHS, other agencies of the federal government, state and local governments, the private sector, and other entities.
- Ensure the timely and efficient access by DHS to all information necessary to discharge the responsibilities contained in Section 201(d) of the Homeland Security Act of 2002, including obtaining such information from other agencies of the federal government.
- Review, analyze, and make recommendations for improvements in the policies and procedures governing the sharing of law enforcement information, intelligence information, intelligence-related information, and other information relating to homeland security within the federal government and state and local governments.
- Disseminate, as appropriate, information analyzed by DHS and IA (1) within DHS, (2) to other federal government agencies relating to homeland security, and (3) to agencies of state and local governments and appropriate private sector entities, in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States.
- Consult with the Director of National Intelligence and other appropriate intelligence, law enforcement, or other elements of the federal government to establish collection priorities and strategies for information relating to threats of terrorism against the U.S. through such means as representation of DHS in discussions regarding requirements and priorities in the collection of such information.
- Consult with state and local governments and private sector entities to ensure appropriate exchange of information relating to threats of terrorism against the U.S.
- Establish and utilize, in conjunction with DHS' chief information officer, a secure communications and information technology infrastructure, including data mining and other advanced analytical tools, in order to accomplish IA's mission.

Collection⁴ of Information About U.S. Persons

In furtherance of I&A's intelligence activities, information about U.S. persons may be collected only when it is necessary for the conduct of I&A's mission and responsibilities and falls within one of the following categories:

⁴ Collection means the gathering or receipt of information, regardless of source, by I&A, coupled with an affirmative act demonstrating intent to use or retain that information for intelligence purposes.

- Information Obtained with Consent. Consent is defined as the voluntary agreement by a person or organization to permit the Office of Intelligence and Analysis to take particular action that affects the person or organization. Consent may be oral or written unless specific by a particular procedure. Consent may be implied if adequate legal notice, as determined by the Office of General Counsel, is provided that a particular action carries with it the presumption of consent to an accompanying action.
- Publicly Available Information. Information is publicly available if it has been published or broadcast for general consumption, is available upon request to a meeting of the general public, could lawfully be seen or heard by a casual observer, or is made available at a meeting open to the general public. In this context, general public also means generally available to persons in the Department, even though the Department is not open to the general public. Information in this category is also called “open source” information.
- Terrorism Information. Terrorism information includes all information relating to the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or transnational terrorist groups or individuals, domestic groups or individuals involved in terrorism, to threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations, or to communications between such groups or individuals reasonably believed to be assisting or associating with them. There must be a reasonable belief of the United States person’s involvement in relation to any use of terrorism information.
- Vulnerabilities Information. Vulnerabilities information includes all U.S. person information required for the assessment of the vulnerabilities of the key resources and critical infrastructure of the United States. Key resources under the Homeland Security Act, section 2(9), means “publicly or privately controlled resources essential to the minimal operations of the economy and government. Critical infrastructure is defined at 42 U.S.C. 5195c(c) as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” Information may be collected about a United States person if there is a reasonable belief in the person’s involvement in relation to any use of vulnerabilities information.
- International Narcotics Activities Information. International narcotics activities are those activities not wholly within the United States to produce, transfer, or sell narcotics or substances controlled in accordance with Title 21, United States Code or those associated activities prohibited by Titles 21 and 46, United States Code. There must be a reasonable belief of the United States person’s involvement in international narcotic activities.
- Border Security Information. Information necessary to protect the safety and integrity of our borders, to include information about United States persons believed to be engaged in illegal activities that cross our borders such as immigration and customs violations. There must be a reasonable belief of the United States person’s involvement in illegal activity that crosses our borders.
- Threats to Safety Information. Information about U.S. persons that is needed to protect the health or safety of any person or organization. Examples include information that may be necessary to identify priorities for either protective security measures or emergency preparedness and response activities, by the Department, other government agencies, the private sector, and other entities.

- **Administrative Information.** Information may be collected about a United States person that is necessary for the function of the Office of Intelligence and Analysis but is not directly related to the performance of intelligence activities. Such information would include DHS personnel and training records, contractor performance records, public and legislative affairs files, and correspondence files maintained in accordance with applicable directives.

Retention⁵ of Information About U.S. Persons

I&A may retain information about U.S. persons, without their consent, subject to the following rules:

- Criteria for retention. Information about U.S. persons is authorized for retention only if it was properly collected. Information about U.S. persons acquired incidental to authorized collection may only be retained if such information could have been collected intentionally.
- Temporary retention. Information about U.S. persons may be retained temporarily, for a period not to exceed 180 days, solely for the purpose of determining whether that information may be permanently retained under these procedures. Once a conclusive determination has been made that information may not be retained, the U.S. person identifying information is to be destroyed immediately.
 - If the information, although not authorized for retention by I&A, is relevant to other agencies' missions, consideration should be given to forwarding the information to those other agencies, consistent with all applicable laws, executive orders, or regulations.
- Access to retained information. Access with I&A to information about U.S. persons shall be limited to those individuals who have a need to know the information in order to perform their official duties.
- Review of intelligence records. I&A shall conduct an annual review of its intelligence records (in whatever form they may be maintained) to evaluate and ensure that continued retention of U.S. person information is necessary to conduct I&A's authorized mission.

Two important caveats to these retention rules: (1) the rules do not apply to information retained solely for administrative purposes or because of an independent legal requirement; and (2) the Freedom of Information Act (5 U.S.C. § 552) and the Privacy Act (5 U.S.C. § 552a) apply to all U.S. person information retained by I&A.

Dissemination⁶ of Information About U.S. Persons

I&A may disseminate information about U.S. persons, without their consent, subject to the following rules:

- Criteria for dissemination⁷. Information about a U.S. person that identifies that person may be disseminated without the consent of that person only if the information was collected and/or

⁵ Retention means the maintenance, storage, synthesis, analysis, production, and other uses short of dissemination, of information about United States persons that can be retrieved by reference to the U.S. person's name or other identifying data.

⁶ Dissemination means the transmission, communication, sharing, or passing of information which has been collected and/or retained pursuant to these guidelines.

⁷ Any dissemination of classified intelligence must be done consistent with E.O. 13292, *Further Amendment to Executive Order 12958, as Amended, Classified National Security Information*, E.O. 12968, *Access to Classified Information*, and E.O. 13388, *Further Strengthening the Sharing of Terrorism Information To Protect Americans*.

retained as discussed above and the recipient of the information is reasonably believed to have a need to receive such information for the performance of a lawful governmental function, such as:

- An employee of a law enforcement intelligence or non-intelligence component of DHS who has a need to know the information to perform his or her official duties;
 - A federal, state, or local law enforcement entity when the information indicates violation of laws enforced by the law enforcement entity;
 - An agency of a state or local government, or a private sector entity with responsibilities relating to homeland security, in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the U.S.
 - An agency within the Intelligence Community, provided that information, other than information collected pursuant to the Foreign Surveillance Act, may be disseminated within the Intelligence Community to each appropriate agency for the purpose of allowing the recipient agency to determine whether the information is relevant to its responsibilities without such a determination being required of the disseminator;
 - A protective, immigration, national defense, or nation security agency of the federal government authorized to receive such information in the performance of a lawful governmental function; or
 - A foreign government and dissemination is undertaken pursuant to an agreement or other understanding with such government in accordance with applicable foreign disclosure policies and procedures.
- In general, U.S. person information slated for dissemination shall not contain the U.S. person's name or other identifying information, unless such data is deemed necessary for the intended recipient to understand, assess, or act on the information provided.
 - Non-publicly available information about U.S. persons obtained through court-authorized electronic surveillance and physical searches should not be provided to state, local, or private sector authorities unless it is confirmed that the information is not FISA-derived, does not concern an U.S. person, or is provided in conformance with court-approved procedures.
 - Other dissemination. Any dissemination that does not conform to the conditions set forth above must be approved by the Assistant Secretary for Intelligence and Analysis after consultation with the DHS Office of General Counsel.

Conclusion

As mentioned above, the guidance contained in this document is designed to serve as a reference tool for all I&A personnel involved in intelligence activities. It does not substitute for legal review of specific intelligence activities and any questions on the applicability or interpretation of this guidance should be directed to the DHS OGC (I&A) legal staff.