Homeland Security

Reports Officer Basic Course

Intelligence Oversight for Reports Officers: Protection of U.S. Person Information in Homeland Intelligence Reports

DHS Office of Intelligence and Analysis

Collection and Requirements Division

Homeland Security

INTRODUCTION

Every member of the Intelligence Community (IC) must comply with rules and regulations governing Intelligence Oversight and the appropriate protection of U.S. Person information.

DHS Reports Officers handle large amounts of information concerning the identities and activities of U.S. persons – far more than most other members of the IC.

This class will cover:

- The history of Intelligence Oversight
- Capabilities and responsibilities of DHS I&A
- Key principles of Intelligence Oversight
- The definition of a U.S. Person
- Specific authorities of DHS I&A
- Procedures for the collection of U.S. Person information
- Exempted categories of information
- Standard guidance for identifying a U.S. Person
- Minimization
- Examples of exemptions codes used in Homeland Intelligence Reports.

Homeland Security

What is Intelligence Oversight?

The process that enables DHS 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 persons.

- Intelligence Oversight is an enabler – not an impediment.
- Requires that decisions to collect, retain and disseminate be made with an informed understanding.
- Reflects our dual obligations – Security and Liberty of US Persons.

Homeland Security

History

Dr. Martin Luther King, Jr.

Civil Rights Movement

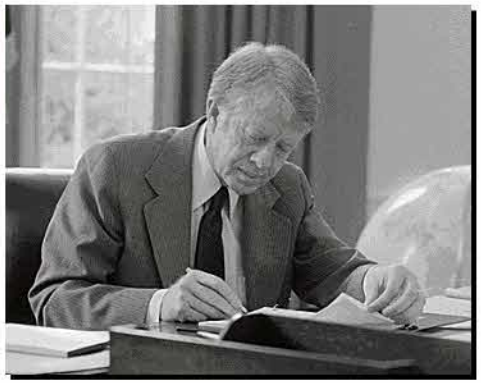
Senator Frank Church Representative Otis Pike

Congressional Hearings

Anti-Vietnam War Movement

President Gerald Ford

E.O. 11905



President Jimmy Carter

E.O. 12036

Homeland Security

IC: Membership Has Its Privileges…

- ★ I&A can access, receive and analyze any type of information
  - National intelligence
  - Terrorism information
  - Law enforcement information
  - Domestic intelligence
  - Other information, such as publicly available
- ★ Information can come from any source
  - Federal Government, State, and local government agencies
  - Private sector entities
  - Individuals

Homeland Security

…And Its Responsibilities!

- Unique rules, policies, and procedures related to intelligence activities
- Increased internal and external oversight of intelligence activities
- Need for specialized DHS policy and training for intelligence professionals

Homeland Security

Key Principles of Intelligence Oversight within DHS

1. Know how to define a U.S. Person (USPER)
2. Ensure intelligence activities fall within the scope of the DHS mission and I&A responsibilities
3. Ensure intelligence activities comply with intelligence oversight guidance for collection, retention, and dissemination
4. Recognize a questionable activity and how to respond to it
5. Understand to whom intelligence oversight procedures apply

Homeland Security

Key Principle 1: What is a "US Person"?

★ **Defined**

1. A United States citizen
2. A lawful permanent resident (green card holder)
3. A group substantially composed of U.S. citizens and/or lawful permanent residents
4. A corporation that is incorporated in the United States
   - A corporation directed and controlled by a foreign government is NOT a U.S. Person
   - A corporation that is incorporated abroad, even if owned by a corporation that is incorporated in the United States, is NOT a U.S. Person

★ **Presumptions**

- ★ Any person or organization found OUTSIDE the United States is presumed to not be a U.S. person, unless there is specific information to the contrary.
- ★ An individual or organization found INSIDE the territorial borders of the United States is presumed to be a U.S. person, unless there is specific information to the contrary.
- ★ Internet Protocol (IP) addresses, uniform resource locators (URLs), and email addresses that are not self evidently associated with a U.S. person may be acquired and processed without making an effort to determine their U.S. Person association as long as no proactive analysis is performed on the addresses. Once analysis is initiated, a reasonable and diligent inquiry must be performed to determine U.S. Person status.

Homeland Security

Key Principle 2: What is the DHS mission?

DHS (Sec. 101 of HSA of 2002):

- **Prevent terrorist attacks within the United States**
- **Reduce the vulnerability of the United States to Terrorism**
- **Carry out functions of legacy agencies**
- **Monitor connections between illegal drug trafficking and terrorism, coordinate efforts to sever such connections, and contribute to interdicting illegal drugs**
- **Ensure that civil rights and civil liberties are not diminished by efforts, activities, and programs**

Homeland Security

Key Principle 2: What are I&A's authorities to support the DHS mission?

Five Authorized Intelligence Activities:

1. Specific Tasks Related to Terrorist Threats

- This category includes a number of specific activities explicitly authorized by law or presidential directive, such as conducting intelligence analysis, facilitating information and intelligence sharing, and establishing and managing collection priorities. All activities performed in this category must relate to terrorist threats to the homeland.

2. General Tasks Related to Priorities for Protective and Support Measures

- This category includes general activities undertaken in furtherance of identifying priorities for protective and support measures by the Department, other agencies of the Federal Government, State and local government agencies and authorities, the private sector, and other entities. An example includes integrating relevant information, analyses, or vulnerability assessments from the Intelligence Community with those from within and outside the Department. All activities performed in this category must relate to actual or potential threats to homeland security
- Threats to homeland security include all threats or hazards, regardless of origin, that relate to: critical infrastructure or key resources; a significant public safety, public health or environmental impact; political, societal and economic infrastructure; border security; the proliferation or use of weapons of mass destruction; or other potential catastrophic events including man-made and natural disasters.

Homeland Security

Key Principle 2: What are I&A's authorities to support the DHS mission?

Five Authorized Intelligence Activities (continued):

3. General Tasks Related to Departmental Support

- This category includes general intelligence and information analysis and support provided to other elements of the Department. All activities performed in this category must be undertaken in furtherance of a lawful activity of the component, such as border security, immigration, or protective activities.
- These are activities undertaken in furtherance of a lawful activity of a component, such as border security, immigration, or protection activities. The most common type of reporting under this activity involves information relating to border security. CBP and ICE play an important role in preventing terrorists, illegal weapons, undocumented aliens, narcotics, agricultural pests and smuggled goods from entering the country. All of these illegal acts fall within the scope of this authority.

4. General Tasks Directed by the Secretary

- Activities undertaken by direction of the Secretary of the Department of Homeland Security. All activities in this category must relate to a responsibility of the Department.

5. Specific Tasks Directed by Statute or Presidential Directive

- Activities required by law or presidential directive, such as providing information in response to judicial discovery or FOIA requests; or providing training to Departmental or other personnel.

Homeland Security

Key Principle 3: Intelligence activities must comply with intelligence oversight procedures for collection, retention, and dissemination

Homeland Security

IO Procedures for collection of USPER

Information that identifies a United States person may be collected by the Office of Intelligence & Analysis if:

1. **It is necessary for the conduct of a function assigned to I&A (i.e., fits within one or more of our five authorities), and;**

2. **It falls within one or more of the following 14 categories:**

Information Obtained with Consent	**Terrorism Information**
Publicly Available Information	**Vulnerabilities Information**
Foreign Intelligence	**International Narcotics Activities**
Counterintelligence	**Border Security Information**
Potential Sources of Assist. to Intelligence Activities	**Threats to Safety**
Protection of Intelligence Sources and Methods	**Overhead Reconnaissance**
Personnel, Physical or Communication Security	**Administrative Information**

Homeland Security

When can I&A collect USPER info?

The Standard

The U.S. Person may be identified when:

(1) The USPER is engaged in an activity covered by one or more of our five authorized intelligence activities; and

(2) The Reports Officer has a "Reasonable Belief" that the information falls within one or more of the fourteen authorized categories for collection.

Applying the Standard

- Subjective Standard

- Based on experience, training, and knowledge as an Intelligence Professional

- Applied to facts and circumstances at hand

- Can be articulated – No Hunches

Minimization

Review I&A products prior to dissemination to determine whether revealing specific U.S. Person information is necessary for the intended recipient to understand, assess, or act on the information provided.

- if not: replace identifier with generic “U.S. Person” or “USPER”

- if so: ensure identifying information is clearly marked and the report contains appropriate warnings

Homeland Security

Key Principle 4: Questionable Activities

- Refers to any intelligence activity that may violate Law, Executive Order or Directive, or Internal DHS Policy
- **REPORTING**:
  - Each individual employee has a responsibility to report
  - Report any questionable activity as soon as you become aware (including proposed activities that may be unlawful)
  - Submit reports to the OGC (Intelligence), IOO, or the IG
  - Breaches of security → CSO / Privacy Violations → CPO

"No adverse action will be taken against any person because that person reports unlawful activities"

Homeland Security

Key Principle 5: Who must follow IO Procedures?

- All I&A personnel (FTEs, Detailees, Contractors)
- Includes those assigned to the NOC (High Side) and any other DHS Component or field activity (e.g., SLFC reps)

Homeland Security

Recap: US Person Information in Homeland Intelligence Reports

- An HIR must report information that is in accordance with a DHS authorized intelligence activity.
- Any U.S. person information included in the HIR must fall within one of the 14 categories of U.S. person information authorized for collection and reporting.
- Each category is assigned a corresponding exemption code that is provided in the HIR.
- Minimization is important and still required.
- When in doubt, err on the side of caution.

Homeland Security

Lessons Learned

Homeland Intelligence Report on Muslim Conference

- A Columbus Ohio police officer noticed a flyer on a local mosque advertising an upcoming conference at a mosque in Atlanta, Georgia entitled “The Best Speech is the Book of Allah”.
- The police officer went on line and found the same flyer posted on the Atlanta mosque website.
- The flyer listed the conference speakers, including a Columbus, Ohio resident who was seen several days later speaking with four individuals outside the Columbus mosque.
- Two of the four individuals had TIDE records.
- HIR written describing the conference, its location, and listing all the speakers, not minimized, and widely disseminated.

Homeland Security

Use of Exemption Codes

- **An analysis of the most commonly used exemption codes follows.**
- **This analysis will not provide an answer to every reportable scenario. Each report must be evaluated independently to determine if an exemption code applies.**
- **The examples contained in this section assume the subject of the HIR is a USPER who does not have a history of reportable activity.**

Homeland Security

Exemption 21: Publicly Available Information

- Information that has been published or broadcast in some manner to the general public; is available upon request to a member of the general public; is accessible to the public; is available to the public by subscription or purchase; could lawfully be seen or heard by a casual observer; is made available at a meeting open to the public; or is obtained by visiting any place or attending any event that is open to the public. Open Source Information is a form of Publicly Available Information. (Note: a website that requires a logon identification and password is not considered publicly available.)
- The RO must demonstrate that the information was obtained through open sources and that the information is necessary for the intended recipient. Publicly available information cannot be used to support an HIR on its own basis. The RO must also be able to explain how the report supports an authorized DHS intelligence activity. If the subject of a report already meets the criteria for a different exemption category, open source material can be used as long as it relates to the incident or activities being reported. Exemption 21 does not provide blanket coverage for all publicly available information.
- **Publicly available information must be used in conjunction with other exemption codes that relate to a specific intelligence activity.**
- Example: If a USPER's name is on a flier advertising a conference, that flier does not, by itself, justify reporting on or naming the USPER. However, if the information on the flier falls within one of the authorized DHS intelligence activities, a report can be drafted.
- Example: If an identified USPER is a TIDE match and can be named under exemption 22, additional information obtained in a public domain, such as an open source website, can be included if it otherwise relates to the information being reported.
- Exemption 21 does NOT apply if there is no derogatory information; or no other reason to suspect an individual is a threat to the homeland; or not otherwise of interest to the Intelligence Community. In such circumstances, open source information about the individual's religious affiliation, employment, etc. cannot be reported under exemption 21.

Homeland Security

Exemption 22: Terrorism Information

- 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.
- Exemption 22 typically requires a TIDE match. However, sometimes Exemption 22 can be used without a direct TIDE match. In these cases, there must be a reasonable belief of the USPER's involvement in relation to any use of terrorism information. U.S. persons who are reasonably believed to be assisting or associating with terrorist groups or individuals may be named under exemption 22. The association must be clearly established and be related to a terrorist activity.
- Example: A person having a conversation with a TIDE match does not establish a reasonable belief of an association. However, if the details of that conversation are known and there is a reasonable belief that the individuals were discussing information related to a terrorist activity, exemption 22 applies.
- Exemption 22 does NOT apply:
  - Children and spouses of TIDE matches are generally not included in HIRs, unless they are TIDE matches themselves.
  - If a subject has a TIDE record and is affiliated with an identified U.S. Organization (USORG), that USORG should not be included in the report unless it also has a TIDE record, or is being nominated for a TIDE record. The subject's standing within the USORG does not affect whether that organization can be named.
  - If a USPER is a TIDE match and is the owner of an identified U.S. business, that USBUS can not be named solely on the basis of its relationship with the USPER. (NOTE: If there is a connection between the USBUS and terrorist activity, the business can be named. For example, if a USBUS is being used to raise money to support terrorist activity, the business can be named under exemption 22.)

Homeland Security

Exemption 23: Vulnerabilities Information

- Information required for the protection of the key resources and critical information of the United States. Key resources under Homeland Security Act, section 2(10), 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(e) 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." These terms are further developed in Homeland Security Presidential Directive 7 "Critical Infrastructure Identification, Prioritization and Protection."
- Exemption 23 can only be used when there is a clearly defined threat to either critical infrastructure or key resources (as defined above). Ultimately though, ROs have a responsibility to clearly identify the location in question as either a key resource or critical infrastructure. For additional definitions, please refer to CRS Study titled "Critical Infrastructure and Key Assets: Definition and Identification" dated 01 October 2004.
- If a clearly defined threat against a piece of critical infrastructure or a key resource exists, the source of the threat or the actual name of the resource or infrastructure should be identified. However, it is vital that the resource in question clearly meets the definition established above.
- When Exemption 23 does NOT apply:
  - Individuals taking photos of bridges do not constitute preoperational planning or a threat per se, nor does a bridge constitute critical infrastructure or a key resource.
  - Reporters must be able to define how something is critical infrastructure or a key resource (like a water treatment plant and the impact it may have).

Homeland Security

Exemption 24: International Narcotics Activities

- ★ Information concerning activities to create, manufacture, distribute, or dispense, or possess with intent to create, manufacture, distribute, or dispense a controlled substance in violation of law, conducted at least in part outside the territorial jurisdiction of the United States.
- ★ Exemption 24 can only be used when the activities are not wholly within the United States. There also must be a reasonable belief of the USPER's involvement in international narcotic activities. This exemption does not only apply to an individual crossing an international border; it also applies to an international narcotics transaction.
- ★ Example: If a USPER admits to crossing the border with narcotics, he/she can be named.
- ★ Example: If there is a reasonable belief that an apprehended USPER was smuggling narcotics which originated in Mexico, the USPER can be named.
- ★ Example: A USPER selling narcotics that were either grown or manufactured outside the United States can be named.
- ★ Exemption 24 does NOT apply:
  - If a USPER is apprehended for narcotics possession near an international border, but there is no evidence that the activities to create, manufacture, distribute, or dispense were conducted at least in part outside the territorial jurisdiction of the United States. The USPER cannot be named.

Homeland Security

Exemption 25: Border Security Information

- Information necessary to protect the safety and integrity of our borders, including information about persons believed to be engaged in activities intended to violate immigration and customs laws and regulations.
- Exemption 25 can only be used when there is a reasonable belief of a USPER's involvement in activities intended to violate immigration and custom laws and regulations. That involvement is not limited to the physical act of crossing the border. If a USPER is involved in some manner with undocumented aliens that recently crossed the border, that USPER can be named if certain criteria have been met.
  - First, the USPER must be aware that he/she is assisting (transporting or housing) an undocumented alien.
  - Second, the USPER's actions must be related to the illegal entry of the undocumented alien. The actions of the USPER must have a direct relationship to the safety and integrity of our borders.
- Exemption 25 also pertains to shipments that cross the border.
  - It is reasonable to assume that a box of fraudulent identifications shipped across the border is a threat to border security.
  - It is also reasonable to assume that a shipment containing fraudulent identification typically used to enter the country is a threat to border security.

Homeland Security

Exemption 25: Border Security Information (continued)

- If a USPER knowingly transports undocumented aliens immediately after they illegally crossed the border, the USPER can be named.
- If a USPER is found to be reportable under this exemption code, but his/her actions occurred months or even years in the past, he/she is still reportable.
- It is important to focus on the actions and operations, rather than the individual. For instance, if a USPER is part of an operation that transports undocumented aliens from one U.S. city to another, that USPER can be named under exemption 25.
- When Exemption 25 does NOT apply:
  - A USPER who gives a ride to an undocumented alien cannot be named unless there is a reasonable suspicion that the USPER was aware of the undocumented alien's status and the USPER intended to violate immigration and customs laws and regulations.
  - A box with fraudulent passports addressed to an identified USPER does not constitute a reasonable belief that the USPER was aware of the shipment's contents…unless a source comment or other information is provided that leads to a reasonable suspicion of the USPER's knowledge or involvement.

Homeland Security

Exemption 27: Threats to Safety

- ★ Information 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.
- ★ A threat to safety, in the context of Exemption 27, may include a U.S. person who is a target, victim, or hostage of a terrorist organization.
- ★ Example: If there is a reasonable belief that a USPER is the target of, or is the victim of, some threat from a terrorist organization, then reporting the identity of the USPER may be done in an attempt to diffuse the threat. The identity of the USPER will be critical for the response.
- ★ When Exemption 27 does NOT apply:
  - Safety is not subject to interpretation. As a result, generic or vague ideas of safety do not apply. A Reports Officer's belief that something is in danger does not give legal authority to identify a USPER.

Homeland Security

US Person Information in HIR Attachments

- Information that could possibly lead to the identification of a USPER should not be included in an attachment to an HIR unless that USPER can be identified under one of the approved exemption codes.
- Examples of this type of information include: driver's license numbers, license plate information, Vehicle Identification Numbers (VIN), telephone numbers, addresses, photographs and fingerprints.
- Lists of telephone numbers will not be included as attachments to HIRs, unless those telephone numbers are known to correspond with entities that should not be treated as U.S. persons.

Some additional Thoughts…

- When you are considering naming a USPER in an HIR, it is best to
  - 1) tie the USPER to a specific nefarious activity or prior bad act pursuant to our authorities, and
  - 2) determine whether the name is needed for the recipient of the HIR to understand, assess, or act on the information provided.
- However, avoid focusing your report on constitutionally protected activities in which the USPER may be involved. Those constitutionally protected activities may be mentioned in a report that focuses on nefarious activities only to provide context for the reader.
- This general rule of thumb applies for known or suspected terrorists, violent domestic extremists, or other adversaries as defined by our updated SINs.

Homeland Security

PRACTICAL EXERCISE 1

Homeland Security

PRACTICAL EXERCISE 2

Homeland Security

PRACTICAL EXERCISE 3

Homeland Security

QUESTIONS?

Homeland Security

UNCLASS//~~FOUO~~

Homeland Security

Additional Slides

Homeland Security

IO Procedure for Retention of USPER

- **RETENTION: The maintenance, including storage, synthesis, analysis, production, and other use short of dissemination, of information about a U.S. Person that can be retrieved by reference to the person's name or other identifying data.**
- **Information may be retained about a U.S. Person if:**
  - **It was intentionally and properly collected; *or***
  - **The information COULD have been collected intentionally.**
- **Information regarding U.S. Persons may not be maintained solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States.**
- **Files containing U.S. Person information must be reviewed annually to determine continued retention.**

Homeland Security

IO Procedure for Temporary Retention

In cases where you are not sure whether the U.S. Person information is covered under one or more of our five authorities for collection and/or the information was obtained from one or more of the fourteen categories for collection...

Temporary Retention: Information about U.S. Person may be retained temporarily, for a period not to exceed 180 days to determine whether the information may be permanently retained

When U.S. Person information may not be retained, it must be DESTROYED IMMEDIATELY (Unless it could be used by another member of the IC)

Homeland Security

IO Procedure for Dissemination of USPER
A Three-Step Process

1. The intended recipient must fit within one of the following three categories:
   - (a) Another member of the IC for whom the information is useful and relevant - in cases where we do not have the authority to retain.
   - (b) An independent legal authority to whom dissemination is required by law.
     (Discovery Requests, FOIA/PA Requests)
   - (c) Federal, State, Tribal, and Local government agencies and authorities, the private sector, and other entities.*

   * As long as there is a reasonable belief that the intended recipient of the information has a need to receive the information for the performance of a lawful governmental or homeland security function, and fits into one of the following categories:
     - DHS Law Enforcement (Intel or Non-Intel) Component
     - Federal, State, Tribal, or Local LEA where info may indicate violation of law under recipient's jurisdiction
     - State, Local or Private Sector entity with Homeland Security responsibilities
     - A Protective, Immigration, National Defense, or National Security Agency of the Federal Government to assist in Performing a Lawful Governmental Function
     - A Foreign Government, pursuant to agreement

Homeland Security

IO Procedure for Dissemination of USPER (cont.)

2. Minimization: Review I&A products prior to dissemination to determine whether U.S. Person info is necessary for the intended recipient to understand, assess, or act on the information provided.

    - if not: replace identifier with generic "a U.S. Person"

    - if so: ensure identifying info is clearly marked "USPER" and document or product contains appropriate warnings

3. Honor other restrictions and controls that may apply to the information.

    - Classified Information Controls

    - Statutory Restrictions on Use (Privacy Act)

    - FISA

    - Agency Policy (ORCON, 3rd Party Controls, Trusted Agent)