DHS Office of Intelligence and Analysis

Intelligence Oversight Training

January 2015

Homeland Security

This briefing contains U.S. PERSON (USPER) information

U.S. Persons: More In-Depth

	U.S. Person	Not a U.S. Person
1) Andrew is a dual U.S. and Canadian citizen.	X	
2) Beth is studying political science at the University of Maryland on a student visa.		X
3) Crayons Inc. is a subsidiary of a German company. Crayons Inc. is incorporated in Delaware.	X	
4) Marilyn Monroe continues to be an American icon.		X
5) A Cadillac Escalade was observed fleeing the scene.		X
6) Preparations are underway for the FedEx Sugar Bowl.		X
7) The abandoned package was located across the McDonald's on Wisconsin Ave. NW.		X
8) The Office of Intelligence and Analysis is part of the Department of Homeland Security.		X
9) Attorney General Eric Holder defends the ruling in a controversial case.		X
10) John was encountered by law enforcement in Akron, OH.	X	

Intelligence Oversight Knowledge Check

1) Which of the following are U.S. persons? Select all that apply.
   a. Andrew, a dual U.S. and Canadian citizen
   c. Crayons Inc., a subsidiary of a German company. Crayons Inc. is incorporated in DE
   e. Eric, an individual encountered by law enforcement in Akron, OH

2) Products or services provided by U.S. businesses are not considered U.S. persons.
   a. True

3) Which of the following statements regarding collection is true? Select all that apply.
   b. Collection is defined as an affirmative action taken by an intelligence professional that demonstrates an intent to use or retain the information for intelligence purposes
   c. DHS I&A may only collect U.S. person information when it is necessary for the conduct of an authorized DHS I&A intelligence activity and the information is reasonably believed to fall into a collection category
   d. DHS I&A may hold U.S. person information for up to 180 days in order to determine whether the information may be retained

4) Which of the following statements accurately depict the reasonable belief standard?
   d. All of the above

Intelligence Oversight Knowledge Check

5) Which of the following are U.S. Person collection categories? Select all that apply.
   c. Vulnerabilities information
   d. Foreign intelligence

6) In order to disseminate intelligence information, DHS I&A personnel must:
   a. Have 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

7) Which of the following may be considered questionable activities? Select all that apply.
   a. Participating in a U.S. organization on behalf of I&A without disclosing one's intelligence community affiliation
   b. Collecting social media that is not publicly available
   c. Tasking state and local law enforcement to collect intelligence information
   d. Collecting U.S. Person information based solely on race, religion, or ethnicity

Intelligence Oversight Knowledge Check

8) U.S. Person information may not be maintained solely for the purpose of monitoring activities protected by the First Amendment.

a. True

9) The Privacy Act:

b. Limits the collection of information that is "relevant and necessary" to accomplish an authorized agency purpose

10) Which of the following statements regarding Personally Identifiable Information (PII) is true?

d. All of the above

Introduction to Intelligence Oversight

- There is an ongoing debate about the breadth of government intrusion into personal privacy in order to enhance security

- Intelligence Oversight enables IC professionals to effectively carry out our authorized functions while ensuring that our activities affecting U.S. persons are conducted in a manner that protects the constitutional rights and privacy of those persons

Introduction to Intelligence Oversight

- Intelligence Oversight applies to:
  - All I&A personnel
    - Feds, contractors, detailees, individuals working on behalf of I&A
  - DHS personnel, regardless of Intelligence Community (IC) affiliation, when performing foreign intelligence or counterintelligence functions

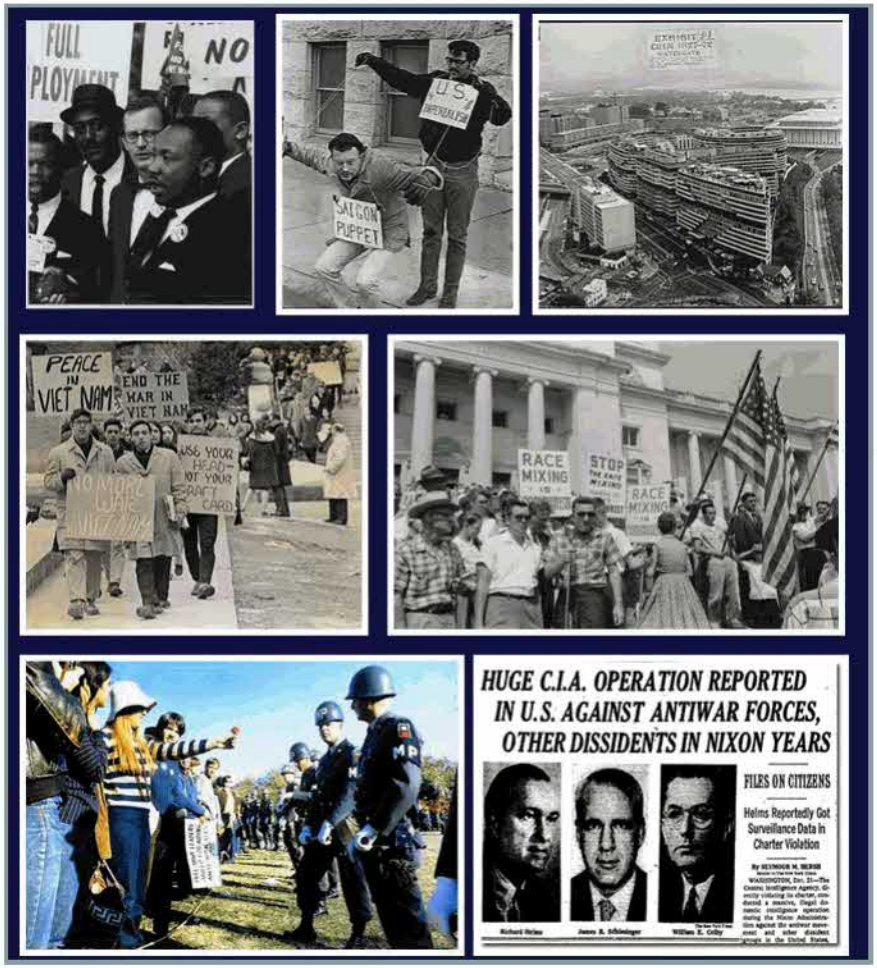
Objectives

- Describe Intelligence Oversight's purpose and history
- Explain Intelligence Oversight requirements and responsibilities for collection, retention, handling, and dissemination of U.S. person information
- Examine questionable intelligence activities and discuss reporting requirements
- Learn about other laws and policies related to privacy

History: Committee Creation

Intelligence activities were conducted with <u>minimal Congressional oversight</u> for most of U.S. history

<u>Mid-1970s:</u> Disconcerting press reporting lead to the creation of the Church and Pike Committees. These committees investigated the legalities of certain Intelligence Community activities which impacted the rights of U.S. persons

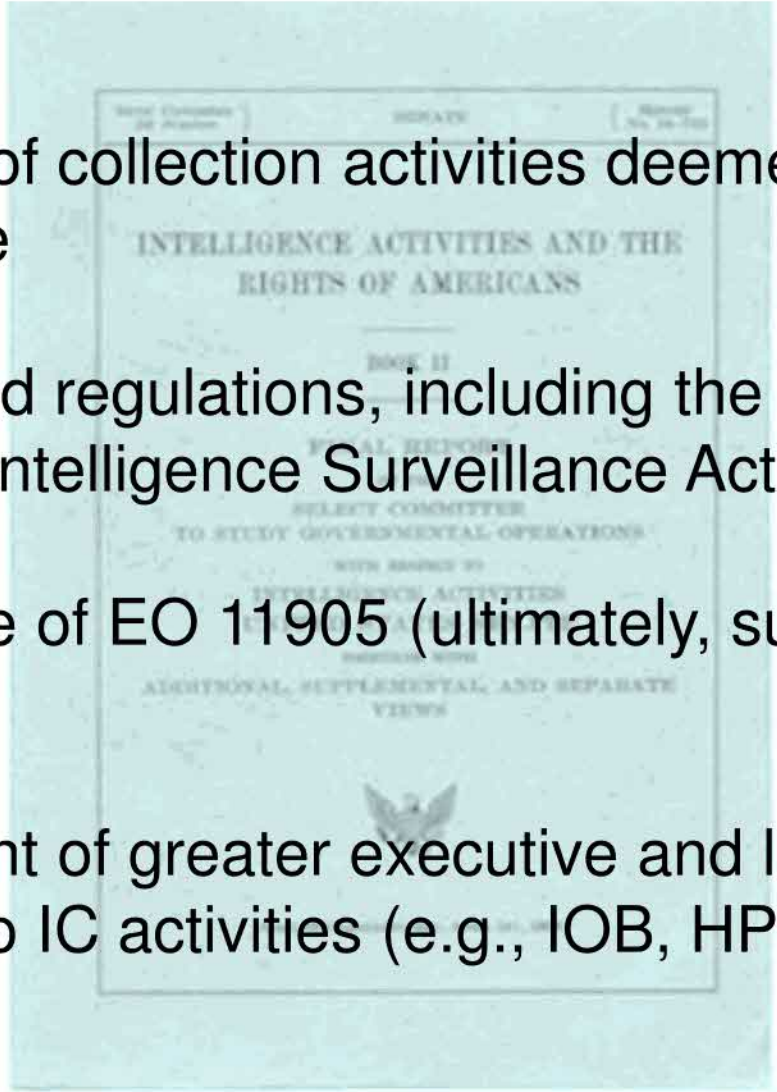


History: Committee Findings

- U.S. person information was improperly collected, retained and disseminated from WW II until the early 1970s
  - Intercepted millions of international telegrams
  - Watchlisted and reported on thousands of "subversives" including political enemies and presumed Communist sympathizers
  - Conducted general phone surveillance in lieu of directed wiretaps
  - Infiltrated women's liberation movement
  - Wiretapped/bugged Dr. King and associates
  - Conducted hundreds of warrantless break-ins

- When properly collected, intelligence is essential
- Beware of evolving technology and times of crisis

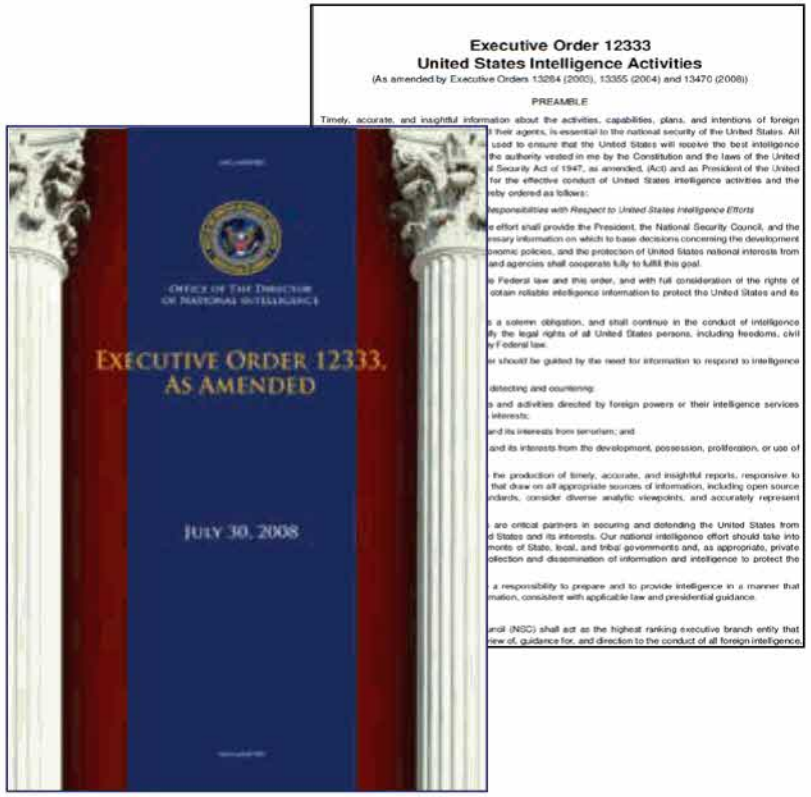
History: Response to Findings



- Termination of collection activities deemed illegal or inappropriate
- New laws and regulations, including the enactment of the Foreign Intelligence Surveillance Act (FISA)
- The issuance of EO 11905 (ultimately, superseded by EO 12333)
- Establishment of greater executive and legislative oversight into IC activities (e.g., IOB, HPSCI, SSCI)

Executive Order 12333: United States Intelligence Activities

The cornerstone document establishing the IC's missions and governing its conduct of intelligence activities



Executive Order 12333

Part 1

"Goals, Directions, Duties, and Responsibilities with Respect to United States Intelligence Activities"

- Specifies the missions and authorities of each IC element

DHS I&A shall collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence and counterintelligence to support national and departmental missions

By contrast, the **CIA** shall collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence

Executive Order 12333

Part 1

"Goals, Directions, Duties, and Responsibilities with Respect to United States Intelligence Activities"

- Specifies the missions and authorities of each IC element

Sec 1.1(g): All departments and agencies have a responsibility to prepare and to provide intelligence in a manner that allows the full and free exchange of information, consistent with applicable law and presidential guidance

Sec 1.4(f): Ensure that all elements within the department or agency comply with the provisions of Part 2 of this order, regardless of Intelligence Community affiliation, when performing foreign intelligence and counterintelligence functions

Executive Order 12333

Part 2

"Conduct of Intelligence Activities"

- Provides principles intended to achieve the proper balance between acquisition of essential information and protection of personal interests

Sec 2.3: Provides categories of information regarding U.S. persons that the IC may collect

Sec 2.4: Requires least intrusive means of collection within the U.S. or directed at U.S. persons abroad

Sec 2.6: Describes circumstances in which the IC may participate in or provide support to LE

Executive Order 12333

Part 2

"Conduct of Intelligence Activities"

- Provides principles intended to achieve the proper balance between acquisition of essential information and protection of personal interests

Sec 2.9: Limits ability to participate in a U.S. organization without disclosing IC affiliation

"No one acting on behalf of elements of the Intelligence Community may join or otherwise participate in any organization in the United States on behalf of any element of the Intelligence Community without disclosing such person's intelligence affiliation"

Executive Order 12333

Part 2

"Conduct of Intelligence Activities"

- Provides principles intended to achieve the proper balance between acquisition of essential information and protection of personal interests

Each IC element must have procedures that implement certain Part 2 of the EO regarding collecting, retaining, or disseminating U.S. person information

These describe how the IC element will use the least intrusive means of collection/support law enforcement, when the IC element can participate in U.S. organizations, etc.

These procedures must be approved by the Attorney General in consultation with the DNI

Interim DHS I&A IO Procedures

UNCLASSIFIED//FOUO

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

April 3, 2008

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

FROM: Charles E. Allen
Under Secretary for Intelligence and Analysis

Matthew L. Kronisch
Associate General Counsel (Intelligence)

SUBJECT: Interim Intelligence Oversight Procedures for the Office of Intelligence & Analysis[1]

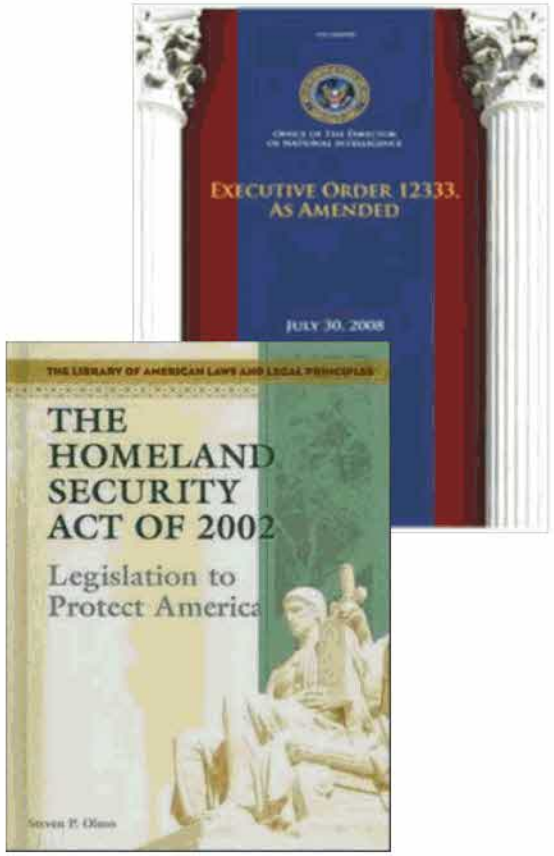
Introduction

The Department of Homeland Security ("DHS" or "Department") Office of Intelligence and Analysis (I&A) is a member of the United States Intelligence Community.[2] 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 Intelligence Oversight is to enable I&A intelligence professionals to effectively carry out their authorized functions while ensuring that their activities affecting U.S. persons[3] are conducted in a manner that protects the constitutional rights and privacy of those U.S. persons and maintains the integrity of the intelligence profession.

Pending approval by the Attorney General of I&A's formal implementing procedures for EO 12333, this document is designed to serve as interim guidance for all I&A personnel (employees, detailees, and contractors supporting I&A) 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 Office of General Counsel (Intelligence).

[1] This memorandum revokes the memorandum, "Intelligence Oversight Basics" dated March 27, 2006.
[2] http://www.intelligence.gov; See also, § 201(h) of the Homeland Security Act of 2002, as amended, the National Security Act of 1947, a amended, 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 know by I&A 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 I&A obtains specific information to the contrary.

UNCLASSIFIED//FOUO



Authorized I&A Intelligence Activities

1. Specific tasks related to terrorist threats
2. General tasks related to priorities for protective and support measures
3. General tasks related to departmental support
4. General tasks directed by the Secretary
5. Specific tasks directed by statute or Presidential directive

New initiatives, or any initiative that impacts constitutionally protected activities, requires prior consultation with the Office of General Counsel (ILD). Any speech or associational activity by a U.S. person or any person on U.S. soil should be presumed to be a constitutionally protected activity.

Authority One: Specific Tasks Related to Terrorist Threats

Section 2 of the Homeland Security Act of 2002, defines "Terrorism" as any activity that:

(A) Involves an act that –

- (i) Is dangerous to human life or potentially destructive of critical infrastructure or key resources; and
- (ii) Is a violation of the criminal laws of the United States or of any State or other subdivision of the United States; and

(B) Appears to be intended –

- (i) To intimidate or coerce a civilian population;
- (ii) To influence the policy of a government by intimidation or coercion; or
- (iii) To affect the conduct of a government by mass destruction, assassination, or kidnapping

Authority Two: General Tasks Related to Priorities for Protective and Support Measures

- Actual or potential threats to homeland security include all threats and hazards, regardless of origin, that relate to:
  - Critical infrastructure/key resources; or,
  - A significant public safety, public health, or other 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

Authority Three: General Tasks Related to Departmental Support

- Provide general intelligence and information analysis and support to other elements of the Department

- Activities must be undertaken in furtherance of a lawful activity of the component, such as border security, immigration, or protective activities

Authority Four: General Tasks Directed by the Secretary

- Perform activities directed by the Secretary in furtherance of an authorized mission of DHS

- These departmental missions are derived from statutory, regulatory, and executive authorities

Authority Five: Specific Tasks Directed by Statute or Presidential Directive

- DHS may be required to undertake specific activities in accordance with a Law or Presidential Directive

U.S. Person Definition

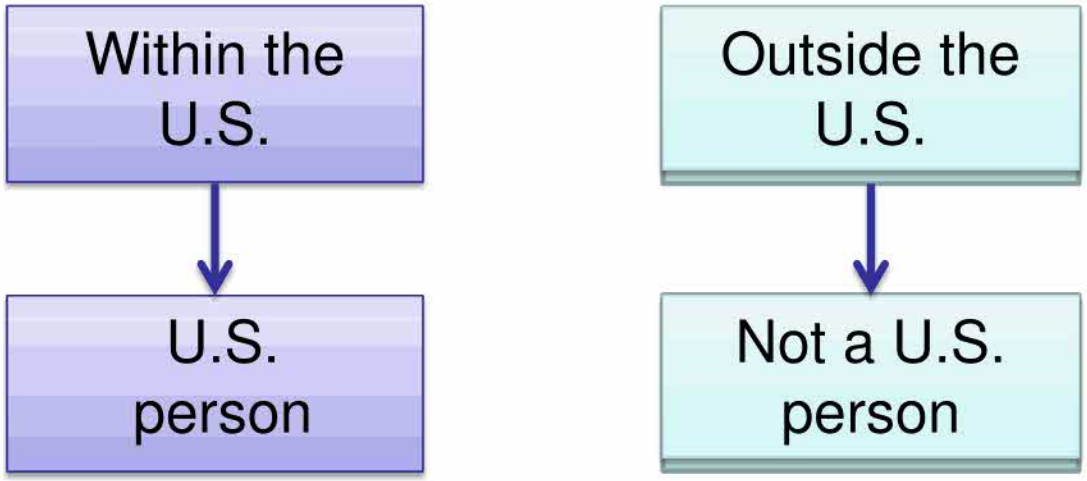
ADDITIONAL INTELLIGENCE OVERSIGHT PROTECTIONS APPLY TO U.S. PERSONS

U.S. persons include:

- U.S. citizens
- Lawful Permanent Residents (LPRs)
- Groups substantially composed of U.S. citizens or LPRs
- Corporations incorporated in the U.S., except for corporations directed or controlled by a foreign government

U.S. Persons: More In-Depth

- Presumptions: Unless there is specific information to the contrary



- U.S. person protections only apply to the living
- Social security numbers, addresses, etc. are not U.S. persons but minimization may apply
- Use good judgment- apply additional protections to juveniles

U.S. Persons: More In-Depth

These are NOT U.S. Persons

- Buildings, laws and events named after U.S. persons
  (e.g., Chrysler Building, Brady Act)
- Names of businesses when used to provide a location
  (e.g., Across from the McDonald's)
- Products and services
  (e.g., Ford Mustang, Twitter, Facebook, The Da Vinci Code)

Context matters in determining U.S. person status

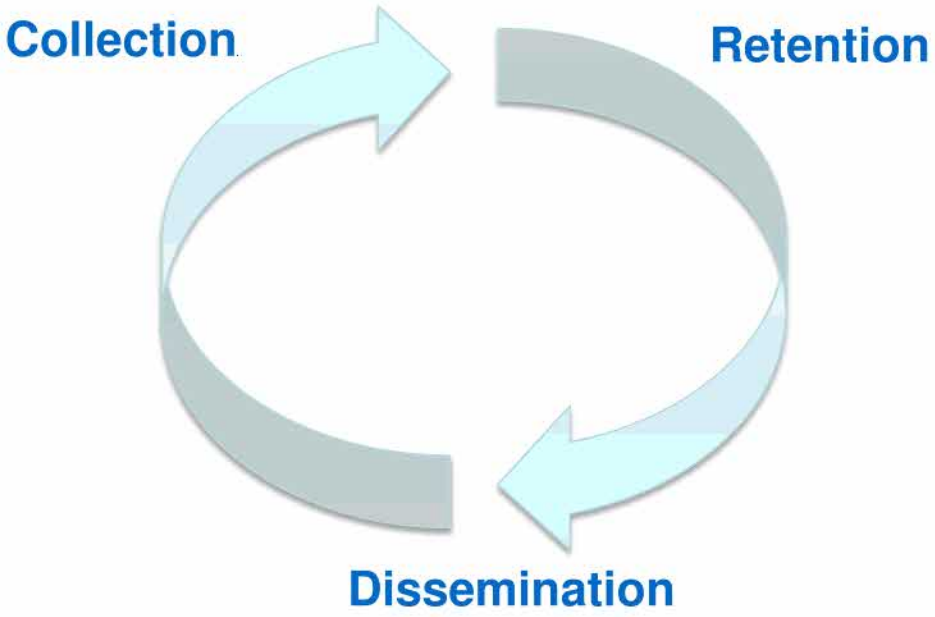
U.S. Persons: More In-Depth

U.S. Person Rules: The Government

- Federal, State and local government agencies and institutions, including public schools, are not U.S. persons
- Generally, government personnel receive U.S. person protections
  - Senior executive branch officials do not receive U.S. person protections when acting in their official capacity
  - Gates Procedures apply to the legislative branch

IO and the Intelligence Cycle

- Intelligence Oversight principles apply throughout the intelligence cycle



Collection

- **Executive Order No. 12333:** Authorizes DHS I&A to "**collect (overtly or through publicly available sources),** analyze, produce, and disseminate" intelligence, counterintelligence and other information that supports "national and departmental missions"

- **I&A's IO Procedure's definition of collection:** When an affirmative action is taken by an intelligence professional that demonstrates an intent to use or retain the information for intelligence purposes

Overt and Publicly Available Information

- **Overt:** The collection of information under circumstances in which the collector's affiliation with the U.S. Government or agency is either openly acknowledged or would be openly acknowledged in response to an express inquiry

- **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

I&A-900 Official Usage Of Publically Available Information

- Open Source Reviewers, describing their roles and responsibilities and training and procedural requirements when conducting open source reviews for RFIs.

- also made changes to ensure PAI collection and dissemination processes are compliant with I&A's Interim Intelligence Oversight Procedures and legal standpoints, specifying requirements for "conducting authorized intelligence activities" and ensuring open source PAI to be used for analytical production is consistent with established policies and guidelines.

You can find this Instruction, along with all approved I&A, Intelligence Enterprise, and Information Sharing and Safeguarding Environment policy-type documents under the "Policy" tab on the top of I&A's homepage.

Collection

I&A may collect only information necessary for the conduct of an authorized intelligence activity

I&A may collect information about U.S. persons only when:

1) Necessary for the conduct of an authorized I&A intelligence activity

AND

2) The information is reasonably believed to fall within a collection category

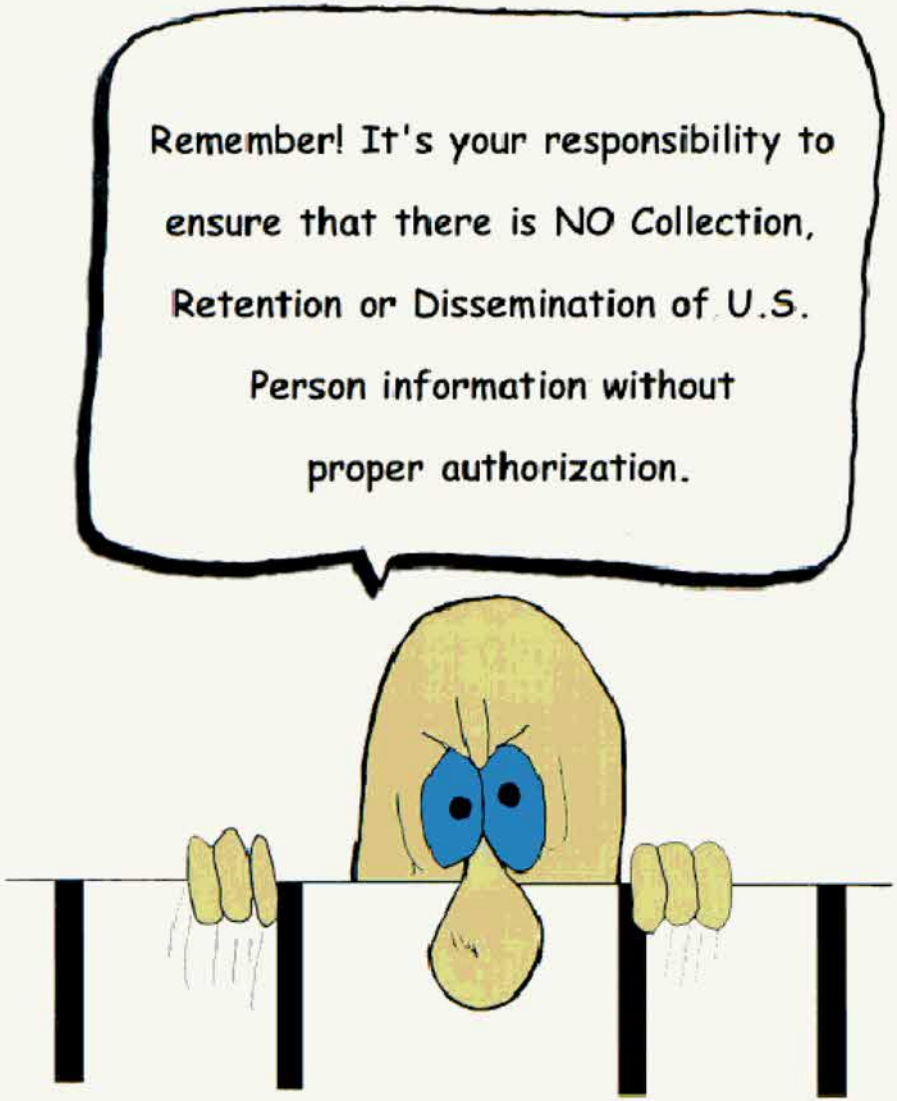
Reasonable Belief

"A reasonable belief arises when the facts and circumstance are such that a reasonable person would hold the belief. Reasonable belief must rest on facts and circumstance that can be articulated; 'hunches' or intuitions are not sufficient. Reasonable belief may be based upon experience, training and knowledge in intelligence or a related field, applied to the facts and circumstances at hand"

Collection Categories

20: Information Obtained with Consent
21: Publicly Available Information
22: Terrorism Information
23: Vulnerabilities Information
24: International Narcotics Activities
25: Border Security Information
26: Administrative Information
27: Threats to Safety
28: Foreign Intelligence
29: Counterintelligence
30: Potential Sources of Assistance to Intelligence Activities
31: Protection of Intelligence Sources and Methods
32: Personnel, Physical or Communications Security
33: Overhead Reconnaissance

INTELLIGENCE OVERSIGHT



Temporary Retention

Uncertain as to whether the U.S. person information meets the two-part standard?

You have 180 days to assess

MEETS THE STANDARD

You can keep the information in accordance with the retention procedures

DOES NOT MEET STANDARD

The information must be destroyed immediately. It may be given to another member of the IC

- *(U)* ***Warning:*** *This product contains US person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It has been highlighted in this document with the label* **USPER** *and should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Other US person information has been minimized. Should you require the minimized US person information, please contact the I&A Production Branch at*

(b)(6)

Retention

- Retention: The maintenance, including storage, synthesis, analysis, production, and other uses 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

  - U.S. person information may not be maintained solely for the purpose of monitoring activities protected by the First Amendment or lawful exercise of other rights secured by the Constitution or U.S. laws

  - Information may be retained about a U.S. person if it was intentionally and properly collected; or could have been collected intentionally

  - Files containing U.S. person information must be marked and reviewed annually to ensure it is within our authorities to retain

Dissemination

- Dissemination: The transmission, communication, sharing, or passing of information outside of I&A. I&A may disseminate U.S. person information:
  - To the IC where we do not have the authority to retain;
  - As required by an independent legal authority (e.g., FOIA request); or
  - To Federal, state, local, tribal, and territorial government agencies and authorities, the private sector, and foreign government (pursuant to agreements) 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

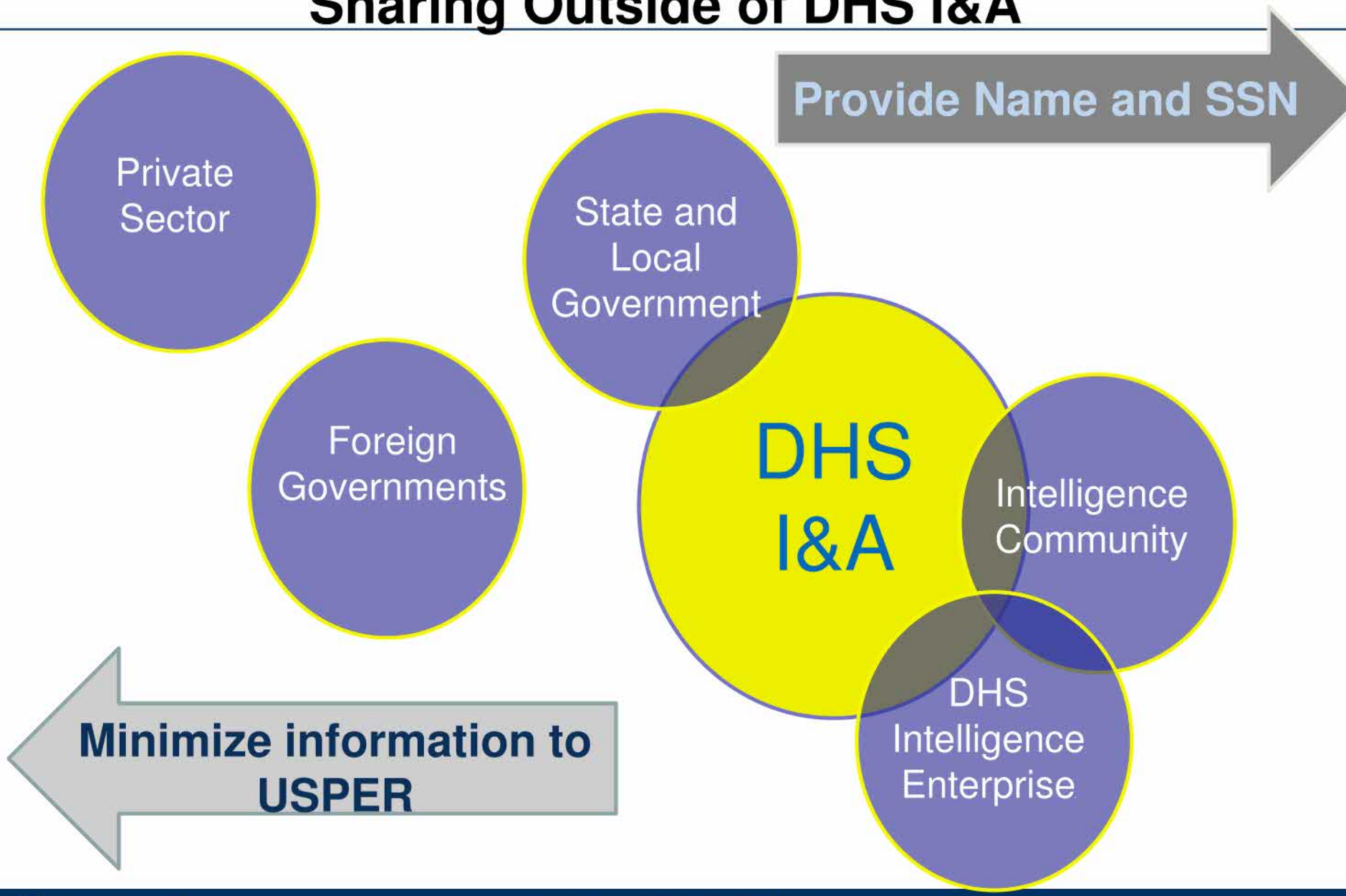
Dissemination: Minimization

Is the U.S. person information necessary for the intended recipient to understand, assess, or act on the information?

YES
Ensure identifying information is clearly marked USPER and include appropriate warnings

NO
Replace identifier with the generic USPER

Sharing Outside of DHS I&A



Open Source Information

- I&A personnel may passively collect, retain and disseminate publicly available information via social media (open source information) for mission-relevant purposes

- Information subject to controlled access is not open source information (e.g., Facebook pages accessible only to certain "friends" or private messaging). I&A is not allowed to directly access this type of information

- I&A personnel may not use personal accounts to collect social media information for I&A use

Questionable Activities

- You are required to report questionable activities to IO, OGC-ILD, or the IG

- Questionable Activity: Any intelligence activity that may violate law, Executive Order, directive, or I&A's Interim Intelligence Oversight Procedures

- Questionable activities will be reported to the Intelligence Oversight Board, as appropriate

Questionable Activities

Examples:

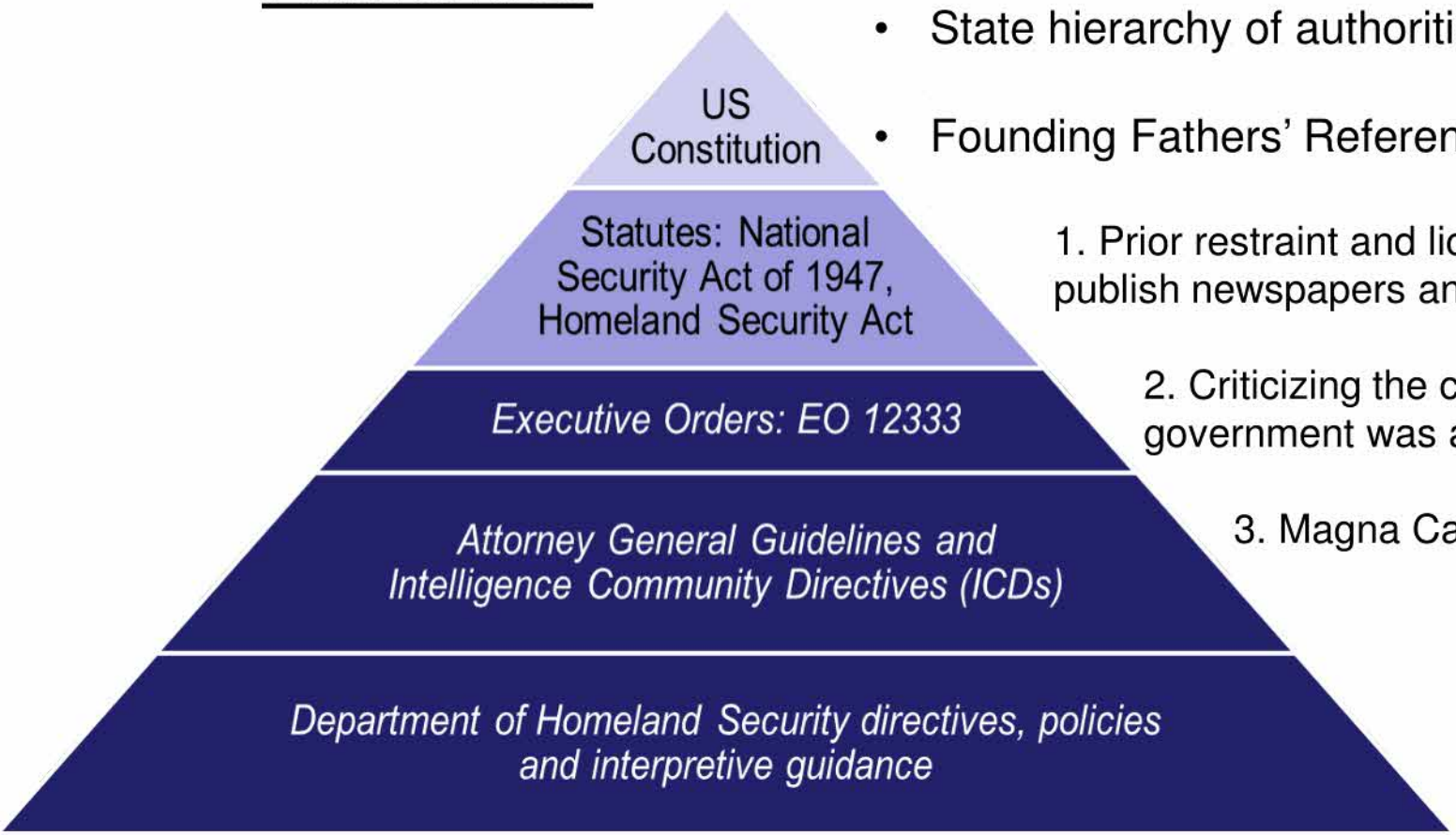
- Tasking someone to conduct intelligence activities that are not part of I&A's mission
- Collecting social media that is not publicly available
- Maintaining U.S. person information for more than 180 days where the information does not meet the two part collection test
- Disseminating intelligence to unauthorized personnel

Additional Laws

- In addition to the U.S. person rules under EO 12333, there are other laws and policies for protecting civil liberties and privacy that govern an IC element's ability to collect, retain, or disseminate information about U.S. persons, including:
  - The Privacy Act
  - The Intelligence Reform and Terrorism Prevention Act (IRTPA), EO 13388, and the ISE Privacy Guidelines
  - Policies issued by the Office of Management and Budget (OMB)

Legal Authorities: Past and Present

The Federal Hierarchy of Authorities



- State hierarchy of authorities runs parallel
- Founding Fathers' Reference Points:

1. Prior restraint and licensing in order to publish newspapers and pamphlets

2. Criticizing the crown and the government was a crime

3. Magna Carta and warrants

Legal Authorities: Constitution

- The word **"privacy"** is not used in the Constitution. However, the courts have interpreted the Constitution to provide protections for privacy-related interests

- **The First Amendment** guarantees freedoms of association, religion, speech, and assembly
  - IC personnel shall not collect/maintain information on U.S. persons solely for the purpose of monitoring protected activities

- **The Fourth Amendment** protects against unreasonable searches and seizures
  - IC personnel should not collect information about a U.S. person that violates a "reasonable expectation of privacy"

- **The Fourteenth Amendment** guarantees equal protection to all persons within U.S. jurisdiction
  - IC personnel shall not collect based solely on race, ethnicity, or religion

The First Amendment

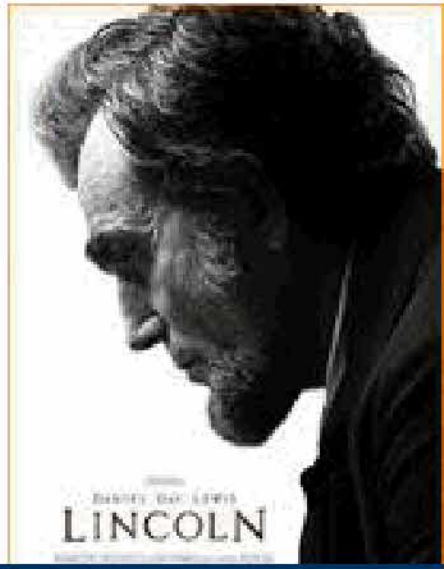
Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances

The Fourth Amendment

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

The Fourteenth Amendment

Section 1. All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws



INTELLIGENCE OVERSIGHT

I want you to protect the constitutional rights of U.S. Persons!

The Privacy Act

- Provides safeguards for individuals against invasions of personal privacy
- Responded to public concerns about government information collection activities
  - Surveillance of civil rights activists
  - Watergate break-in
  - IRS tax records
- Protects against the release of information without the individual's consent or a statutorily authorized condition, including the agency's published "routine uses"
- Applies to federal agencies' system of records about individuals.

The Privacy Act: Definitions

- Individual: U.S. citizen or LPR (different from EO 12333 "U.S. person," which includes organizations)

- Record: Any item, collection, or grouping of information containing the individual's name, identifying number, symbol, or other identifier (e.g., fingerprint or photograph)

- System of Records: Grouping of records from which a federal agency retrieves information by the individual's name or by a unique identifier assigned the individual

The Privacy Act: Essentials

– **Notice:**

- Agencies must publish a Systems of Records Notice (SORN) in the Federal Registrar, describing the compilation of records and purpose for the collection

- Agencies collecting information from the individual must provide a Privacy Act Statement/Notice of Collection

The Privacy Act: Essentials

- **Access and Amendment:** Subject to exceptions, such as national security, individuals are entitled to review and correct records maintained about them

- **Minimum Necessary:** Limited to the collection of information that is "relevant and necessary" to accomplish an authorized agency purpose

- **Data Quality:** Reasonable effort to ensure records are as timely, relevant, accurate and complete as necessary for the purpose that they were collected

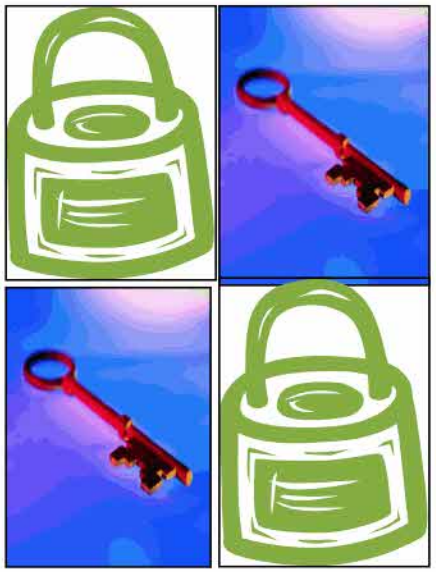
The Privacy Act: Essentials

- **First Amendment Protection:** Absent authorized law enforcement activity

- **Safeguards:** Technical and administrative to ensure security, confidentiality, integrity, and availability

- **Penalties:**
  - Civil Penalties for violations of administrative and technical requirements
  - Criminal Penalties for knowingly and willfully disregards notice requirements or prohibitions on disclosure

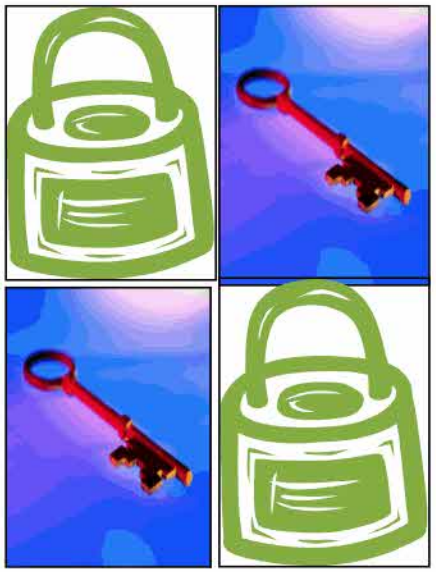
Laws with Privacy Implications



- The E-Government Act of 2002
  - Blends privacy protections with IT security
  - Requires Privacy Impact Assessments (PIA) of Information Technology Systems

- The Homeland Security Act of 2002
  - Creates the first statutory Chief Privacy Officer and Privacy Office
  - Broadens the PIA requirement
  - Adds Privacy Threshold Analysis (PTA) requirement for National Security Systems

Laws with Privacy Implications



- Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)
  - Charges the president to create a terrorism information sharing framework that honors applicable legal standards that relate to privacy and civil liberties

Guidance on PII: OMB Memoranda

- OMB M-07-16: Personally Identifiable Information (PII) is information that can be used to distinguish or trace an individual's identity alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual

- OMB M-10-22: Some PII is more sensitive than other PII. If Sensitive PII (SPII) is compromised, it could cause practical harm (e.g., economic, reputational or physical harm)

DHS Guidance on Sensitive PII

- DHS Handbook for Safeguarding Sensitive Personally Identifiable Information, March 2012: Sensitive PII is PII that, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

What is PII and Sensitive PII?

PII includes:

Name, email, work address, phone number

Sensitive PII includes:

If Stand-Alone:	*If Paired With Another Identifier:*
➢ Social Security number	➢ Citizenship or immigration status
➢ Diver's license or state ID number	➢ Medical information
➢ Passport number	➢ Ethnic or religious affiliation
➢ Alien Registration Number (ARN)	➢ Sexual orientation
➢ TIDE Person Number (TPN)	➢ Account passwords
➢ National Unique Identification Number (NUIN)	➢ Last 4 digits of SSN
➢ Financial account number	➢ Date of Birth
➢ Biometric identifiers	➢ Criminal history
	➢ Mother's maiden name

Consequences of Not Protecting PII

For DHS:

- Loss of public trust
- Increased Congressional oversight
- Loss of funding

For the victim:

- Identity theft
- Loss of benefits
- Embarrassment

For the person causing the incident:

- Counseling and training
- Loss of employment
- Civil & criminal penalties

The Washin

Friday, April 13, 2010

DHS Data Breached

Due to employee mishandling, personal information on 10,000 DHS employees was lost.

Employees fear that they will be victims of identity theft.

Ren
foll
imp

Guidance on PII: OMB Memoranda

- OMB M-06-15: Directs agencies to safeguard PII through technical, administrative and physical controls and to establish procedures and restrictions on the use or removal of PII beyond agency premises or control (e.g., mobile devices)

- OMB M-07-16: Directs agencies to establish incident response procedures to assess and mitigate potential harm to individuals from unauthorized use or disclosure of PII

*** Report unauthorized disclosures of PII immediately ***

How to Safeguard SPII

Emailing SPII

- Create separate document to be attached
- Password-protect the document
- Send password in separate email

Destroying SPII

- SPII must be properly disposed when no longer required
- Notify Help Desk to sanitize SPII from electronic devices before transferring equipment to other users

Intelligence Oversight Staff

- Review intelligence products
- Provide annual Intelligence Oversight training
- Report to the Intelligence Oversight Board (IOB)

- Shared Mailboxes:

(b)(6)

- DHS Connect SharePoint:

(b)(6)

Course Summary

- The underlying principles of Intelligence Oversight apply to all IC elements
- EO 12333 and the IC element's Attorney General Approved Guidelines govern the collection, retention, and dissemination of information about U.S. persons
- Additional statutory and regulatory requirements protect privacy and civil liberties