

UNCLASSIFIED



**OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**  
LEADING INTELLIGENCE INTEGRATION


## Why We Are Here

- Intelligence Community (IC) professionals take an **OATH** to carry out the missions of their agencies in accordance with the Constitution and laws
- EO 12333 requires that we execute our **NATIONAL SECURITY MISSION** *in a manner that protects fully the freedoms, civil liberties and privacy rights of US persons*
- Protecting these **FREEDOMS, CIVIL LIBERTIES AND PRIVACY RIGHTS** fosters trust from the public, our mission partners and other stakeholders that we properly use and protect the data they provide to us
- **TRUST** is critical to our efforts to protect national security. Without trust in our IC institutions, processes and leaders, we risk losing access to data and authorities vital to accomplishing our national security mission
- Collecting, handling, sharing and safeguarding US Person information lawfully and consistently across the IC is therefore **ESSENTIAL** to achieving the IC's missions and goals

2

UNCLASSIFIED

UNCLASSIFIED



**OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**  
LEADING INTELLIGENCE INTEGRATION

## Course Goals


- Understand the IC's dual mandate to provide timely and relevant intelligence AND to protect the privacy rights and civil liberties of US Persons
- **Module 1:** Understand the basic rules under EO 12333 regarding the collection, retention and dissemination of US Person information
  - Definition of US Person
  - Types of US Person information that may be collected and shared
- **Module 2:** Understand other relevant civil liberties and privacy rules
  - Privacy Act, Foreign Intelligence Surveillance Act (FISA), Office of Management and Budget (OMB) regulations, Information Sharing Environment (ISE) Privacy Guidelines

3


UNCLASSIFIED

UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION



# Module 1




- *Framework of EO12333*
- *Definition of US Person*
- *Attorney General-Approved Implementing Guidelines*

4

UNCLASSIFIED

UNCLASSIFIED



**OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**  
LEADING INTELLIGENCE INTEGRATION

## Module Objectives

- Understand the US Person framework in EO 12333
- Appreciate how the IC's history has shaped the laws and practices governing the collection, retention and dissemination of information concerning US Persons
- Understand that US Person information may be collected, retained, or disseminated when:
  - consistent with the element's mission;
  - justifiable under an authorized EO 12333 category of collection; and
  - permissible under the element's Attorney General (AG)-approved implementing guidelines

5

UNCLASSIFIED

See authorized categories of collection on slides 15-16.

AG-approved guidelines and procedures can expand on EO 12333 Part 2.3 listing of categories of information that the IC may collect.

UNCLASSIFIED

**OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**  
LEADING INTELLIGENCE INTEGRATION

**Domestic Intelligence Collection:  
Congressional Investigations**

- In 1975 and 1976, Congress investigated the IC's domestic intelligence activities
  - The Senate's Church Committee
  - The House's Pike Committee

“Domestic intelligence activity has threatened and undermined the Constitutional rights of Americans to free speech, association and privacy. It has done so primarily because the Constitutional system for checking abuse of power has not been applied.”

~ Church Committee Final Report


Source: ...

UNCLASSIFIED

## Domestic Intelligence Collection

- Truman through Nixon Administrations – provided vague intelligence collection guidance that led to:
  - Mail openings
  - Break-ins
  - Medical experiments
  - Smear campaigns
- These violations prompted Congressional investigations

UNCLASSIFIED



**OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**  
LEADING INTELLIGENCE INTEGRATION

## Church/Pike Investigations

- NSA surveillance:
  - Intercepted and reviewed millions of international telegrams
  - Watch-listed and reported on thousands of allegedly “subversive” Americans
  - Conducted general phone surveillance in lieu of directed wiretaps on targets
  
- FBI surveillance:
  - Wiretapped lobbyists, political enemies, presumed Communist sympathizers
  - Infiltrated women’s liberation movement
  - Investigated NAACP for 25 years; wiretapped/bugged Dr. King and associates
  - Conducted hundreds of warrantless break-ins
  
- CIA activities:
  - Provided covert support to military coups/assassinations around the world

7

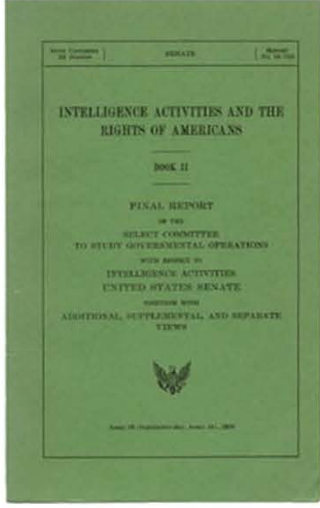
UNCLASSIFIED



UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION

## Sample Conclusions (from Church/Pike)



The image shows the front cover of a green report. The text on the cover reads: 'INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS', 'BOOK II', 'FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES UNITED STATES SENATE', 'INCLUDING WITH ADDITIONAL, SUPPLEMENTAL, AND SEPARATE VIEWS'. There is a small eagle emblem at the bottom center.

- **Intelligence is essential**
  - “[T]he power of government to conduct *proper* domestic intelligence activities under effective restraints and controls must be preserved.”
- **Beware of times of crisis**
  - “In time of crisis, the Government will exercise its power to conduct domestic intelligence activities to the fullest extent.”
- **Technology and Big Brother**
  - “In an era where the technological capability of Government relentlessly increases, we must be wary of the drift toward ‘big brother government.’”
- **Protect Privacy and Civil Liberties**
  - “[T]oo often ... domestic intelligence activities have invaded individual privacy and violated the rights of lawful assembly and political expression.”


8

UNCLASSIFIED



UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION



## Domestic Intelligence Collection: Response to Congressional Investigations

- The original version of what became EO12333 was written, in part, in response to the Church/Pike committees findings
- While the EO has been amended several times, its protections for the freedoms, civil liberties and privacy rights of US Persons have remained essentially unchanged
- Church/Pike committees became the permanent intelligence oversight entities in the Senate and House

9

UNCLASSIFIED

### Govt Response: Mid 70s – 1981

- System of Executive Branch rules established
  - EO 11905 under President Ford.
    - Established an Intelligence Oversight Board to receive reports regarding “activities that raise questions of legality or propriety”
  - Later replaced by EO 12036 under President Carter
  - then EO 12333 under President Reagan

**E.O. 11905, and 12036:** “The measures employed to acquire [intelligence] information ... must be conducted in a manner that **preserves and respects established concepts of privacy and civil liberties.**”

- Offices of General Counsel and intelligence oversight functions enhanced
- Intelligence Oversight Board established in EO 11905 to receive reports regarding “activities that raise questions of legality or propriety”
- Congressional Oversight Committees established
  - Senate Select Committee on Intelligence (SSCI)
  - House Permanent Select Committee on Intelligence (HPSCI)
- Statutory framework for electronic surveillance for national security
- Legislation passed
  - *The Privacy Act*
  - *FISA*


UNCLASSIFIED

**OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**  
LEADING INTELLIGENCE INTEGRATION

**EO 12333**

"Executive Order 12333 is a cornerstone document for the Intelligence Community. The Executive Order sets strategic goals and defines roles and responsibilities within the Intelligence Community, while also affirming the Nation's commitment to protect Americans' civil liberties and privacy rights in the conduct of intelligence activities."

~White House Press Release  
on the 2008 Revision



10

UNCLASSIFIED



UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION

## EO 12333 - Structure

EO 12333 has three main parts

Part 1	Part 2	Part 3
<p><i>"Goals, Directions, Duties, and Responsibilities with Respect to United States Intelligence Activities"</i></p> <ul style="list-style-type: none"> <li>• Specifies the missions and authorities of each IC element</li> </ul>	<p><i>"Conduct of Intelligence Activities"</i></p> <ul style="list-style-type: none"> <li>• Provides principles intended to achieve the proper balance between acquisition of essential information and protection of personal interests</li> </ul>	<p><i>"General Provisions"</i></p> <ul style="list-style-type: none"> <li>• Contains definitions</li> </ul>

12

UNCLASSIFIED

Part 1 of EO 12333 sets the tone of the IC and details the following:

- Goals of the IC
- Role and duties of the National Security Council (NSC), Director of National Intelligence (DNI), and the Heads of IC elements
- IC elements and their authorities regarding intelligence activities


Note that the heads of *all* Executive Branch agencies have duties and responsibilities to support the DNI's intelligence mission (see Part 1.5)

Part 2 details the purposes and techniques for collection of intelligence by the various IC elements. (e.g., the need for AG approval to surveil or monitor w/in the US or against a USP abroad; prohibition on undisclosed participation in organizations in the US unless the organization is composed primarily of non-USPs and is reasonably believed to be acting on behalf of a foreign power).

Part 3 of EO 12333 provides definitions of essential terms and concepts:

- USP
- Intelligence (i.e., National Intelligence, Intelligence Related to National Security, National Intelligence Activities, and Foreign Intelligence)
- Intelligence Activities
- Intelligence Community

UNCLASSIFIED



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION

## EO 12333 / Part 1


### Agency Mission Examples

- **CIA:** coordinates clandestine collection of foreign intelligence through “human sources or through human-enabled means” *outside of the US*
- **FBI:** coordinates clandestine collection of foreign intelligence through “human sources or through human-enabled means” *inside the US*
- **DOD:** conducts programs and missions to fulfill national, departmental, and tactical intelligence requirements
- **NSA:** possesses primary authority to engage in signals intelligence activities

13

UNCLASSIFIED

UNCLASSIFIED



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION

## EO 12333 / Part 2

### Collection Rules Examples


- **Part 2.3:** describes categories of information regarding US Persons that the IC elements are authorized to collect
- **Part 2.4:** requires least intrusive means of collection within the US or directed at US Persons abroad; prohibits surveillance/monitoring except in specific circumstances
- **Part 2.6:** describes circumstances in which IC element may participate in or provide support to law enforcement
- **Part 2.9:** limits ability to participate in a US organization without disclosing IC affiliation

14

UNCLASSIFIED

UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION



## EO 12333 / Part 3 Definitions

- **Intelligence activities:** all activities that elements of the Intelligence Community are authorized to conduct pursuant to EO 12333
  
- **Foreign intelligence:** information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists
  
- **National Intelligence and Intelligence Related to National Security:** all intelligence, regardless of the source ... gathered within or outside the United States, that pertains ... to more than one United States Government agency; and that involves threats to the United States, its people, property, or interests; the development, proliferation, or use of weapons of mass destruction; or any other matter bearing on United States national or homeland security.

15

UNCLASSIFIED




UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION

**Definitions Cont'd**  
**US Person (USP)**

US Person (USP) is:

- A US citizen,
- An alien known by the intelligence agency element concerned to be a permanent resident alien (i.e., lawful permanent resident, green card holder),
- An unincorporated association substantially composed of US citizens or permanent resident aliens, or
- A corporation incorporated in the US, except for a corporation directed and controlled by a foreign government or governments.



16

UNCLASSIFIED

#### USP examples:


- Person born in the U.S. or naturalized as a citizen
- Person with dual citizenship
- Green card holder
- Not for profit group or social club substantially composed of USPs
- US legal corporation
- US legally established subsidiary of a foreign (non-government) corporation

#### Non-USP examples:

- Foreign citizen
- Visa holder
- Foreign corporation even if doing business in US
- Or foreign government directed/controlled
- Foreign legal US subsidiary (incorporated/legally formed under foreign law)

Presumption: a person encountered in the US, its territories and possessions is presumed to be a USP unless there is evidence to the contrary

UNCLASSIFIED



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION

## Responsibility to Provide

EO 12333, Part 1.1(g) dictates that all departments and agencies have a responsibility to prepare and provide intelligence in a manner that allows the full and free exchange of information, consistent with applicable law and presidential guidance

“Responsibility to provide” as balanced against “need to protect” is also echoed in ICD 501 and ICPM 2007-200-2

17

UNCLASSIFIED


“Responsibility to Provide” is in tension with the “need to protect.” While driving intelligence -- through mission imperatives and sound intelligence tradecraft to serve its customers -- the IC must balance the risk of providing information with the need to protect sources and methods. (ICPM 2007-200-2)

Additionally ICD 501 establishes that IC elements shall treat information collected and analysis produced as national assets and, as such, shall act as stewards of information who have a predominant “responsibility to provide.”

Note that responsibility to provide must be “consistent with applicable law and presidential guidance,” so – for example – a particular minimization provision governing dissemination in FISA cases might preclude providing intelligence n/w/s the mandate.

UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION



## Criteria for Collection, Retention, and Dissemination of USP Information

**Categories of US Person information that may be collected, retained, or disseminated IF consistent with the IC element's mission AND accomplished in accordance with the element's Attorney General-approved procedures:**


- Information that is publicly available or collected with the consent of the person concerned
- Foreign intelligence or counterintelligence information
- Information obtained in the course of a lawful foreign intelligence, counterintelligence, international drug or international terrorism investigation
- Information needed to protect the safety of persons or organizations
- Information needed to protect foreign intelligence or counterintelligence sources, methods, and activities from unauthorized disclosure
- Information concerning potential sources or contacts for the purpose of determining their suitability or credibility

18

UNCLASSIFIED

UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION



## Criteria for Collection, Retention, and Dissemination of USP Information (cont'd)

**Categories of US Person information that may be collected, retained, or disseminated IF consistent with the IC element's mission AND accomplished in accordance with the element's Attorney General-approved procedures:**

- Information arising out a lawful personnel, physical, or communications security investigation
- Information acquired by overhead reconnaissance not directed at specific US Persons
- Incidentally acquired information that may indicate involvement in activities that may violate federal, state, local, or foreign laws
- Information necessary for administrative purposes (HR, contracting information, etc.)


19

UNCLASSIFIED

Note again that dissemination of USP information could be trumped by a FISA minimization provision that is more restrictive.

UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION



## Attorney General's Guidelines

- EO 12333 requires each IC element to have procedures implementing Part 2 of the EO regarding collecting, retaining, or disseminating US Person information
- These procedures must address all matters covered by Part 2 of the EO as they will be implemented by the specific element under its unique authorities: e.g., as regards use of certain collection techniques, conduct of physical surveillance (if permissible), provision of support to law enforcement and civil authorities (circumstances), and participation in organizations without disclosing IC affiliation
- These procedures must be approved by the Attorney General in consultation with the DNI

20

UNCLASSIFIED

“Elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only **in accordance with procedures** established by the head of the Intelligence Community element concerned or by the head of a department containing such element and **approved by the Attorney General** consistent with the authorities provided by Part 1 of this order, after consultation with the Director.”


EO 12333, 2.3

AG Guidelines, e.g.:

- Department of Defense (DoD) Directive 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect U.S. Persons
- Attorney General's Guidelines for Domestic FBI Operations

UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION



## Dissemination inside and outside the IC

- Information may be disseminated, but the HOW depends on whether inside or outside the IC. For example:
  - *If inside the IC:* To other appropriate IC elements so they can determine if relevant to their mission; or finished information in accordance with disseminator's AG-approved implementing guidelines
  - *If outside the IC:* Finished information where recipient agency has a need for the information in the performance of a lawful function, and sharing is consistent with disseminator's AG-approved implementing guidelines


21

UNCLASSIFIED

Note that the standards for disseminations inside/outside the IC may not be consistent with a FISA minimization provision for a particular agency or a particular agency's AG guidelines dissemination provision.

Note also: E.O. 12333 prescribes a more restrictive approach for SIGINT (may only be disseminated or made available to IC elements in accordance with procedures established by the DNI in coordination with the Secretary of Defense and approved by the AG)

UNCLASSIFIED



**OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**  
LEADING INTELLIGENCE INTEGRATION

## Module Summary

- EO 12333 is a cornerstone document that defines the IC elements' missions, authorities and responsibilities, and lays out rules to protect US Persons' privacy and civil liberties.
- The definition of a US Person includes:
  - US citizens
  - Permanent resident aliens
  - Unincorporated organizations substantially composed of US citizens and permanent resident aliens, and
  - Organizations incorporated in the US
- US Person information may be collected, retained, or disseminated if consistent with the element's mission; consistent with an authorized category of collection; and permissible under the element's AG-approved guidelines


22

UNCLASSIFIED




UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION



## Module 2




Module 2

- *An Overview of Other Laws and Policies Protecting Civil Liberties and Privacy in the Collection, Retention or Dissemination of Information*

23

UNCLASSIFIED

UNCLASSIFIED



**OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**  
LEADING INTELLIGENCE INTEGRATION

## Module Objective

- In addition to the US 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 US Persons, including:
  - The US Constitution
  - The Foreign Intelligence Surveillance Act (FISA)
  - 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)

24

UNCLASSIFIED


Please note that this list is not exhaustive.



US Constitution: Establishes powers and duties of the three Branches of government and sets out individual rights vis a vis the government

Laws: Authorize and fund activities of the Federal Government (among other things)

UNCLASSIFIED

 OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION

## The US Constitution

- The word "privacy" is not used anywhere in the Constitution. However, the courts have interpreted the Constitution to provide protections for privacy-related interests.
- **First Amendment:** Guarantees freedoms of association, religion, speech, and assembly.
  - IC personnel should not collect/maintain information on US Persons solely for the purpose of monitoring activities protected by the First Amendment or other lawful activities.
- **Equal Protection (Fourteenth Amendment):** Guarantees equal protection to all persons within US jurisdiction.
  - IC personnel should not collect information about a person or group based solely on race, ethnicity, or religion.
- **Fourth Amendment:** Guarantees freedom from "unreasonable searches and seizures."
  - IC personnel should not collect information about a US Person that violates a "reasonable expectation of privacy." The courts have identified a reasonable expectation of privacy in telephone conversations, computer content, and activities occurring in one's home.
  - Special authorization (e.g., court order) is required to obtain information protected by the 4<sup>th</sup> Amendment, whether in the US or abroad.

26

UNCLASSIFIED


Fourth Amendment requires Court approval for use of electronic surveillance, non-consensual physical searches, etc. for intelligence purposes within the US or against a USP abroad.

UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION

**The Foreign Intelligence Surveillance Act (FISA)**

- FISA (passed in 1978) established:
  - Requirement to seek judicial approval before conducting electronic surveillance in the US to obtain foreign intelligence (e.g., tap a phone)
  - The Foreign Intelligence Surveillance Court (FISC) to determine whether there is **probable cause** to believe that the target is a foreign power or an **agent of a foreign power (includes Foreign Terrorist Organizations)**
- FISC approval procedure subsequently extended to:
  - Physical searches (1994)
  - Pen register/trap & trace devices (phone dialing and routing information) (1998)
  - Access to certain business records (2001)
  - Targeting non-USPs outside the US (2008)
    - No probable cause showing for non-USP (Under 702)



27


UNCLASSIFIED

Recall that FISA was outgrowth of Church/Pike hearings on politically-motivated surveillance

Distinguish FISA surveillance from Title III wiretaps --- purpose is foreign intelligence versus criminal investigatory purpose

By distinction, the targeting of non USPs outside the US is authorized under the FISA Amendments Act of 2008 (FAA) – requires the AG and DNI to approve certifications, which the FISC in turn must approve. Statement of probable cause not required, as in the other FISA activities. Lower expectation of privacy by non-nationals outside of the US.

UNCLASSIFIED



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION

## FISA Surveillance/Search

**Probable cause** regarding the object of search/surveillance:

**Electronic surveillance:**

- Facilities or places are being used or are about to be used by the target

**Physical search:**

- Premises or property contains foreign intelligence information
- Premises or property is or is about to be owned, used, possessed by, or is in transit to or from the target


(See FISA Titles I and III)

28

UNCLASSIFIED

UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION



## FISA Pen Register/Trap and Trace and Business Records

**Pen register/trap and trace:**

Application must certify that information likely to be obtained is:

- Foreign intelligence information not concerning a USP, **OR**
- Relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a USP is not conducted solely upon the basis of activities protected by the First Amendment

**Business records:**

Application shall include facts showing that there are reasonable grounds to believe that:

- Tangible things sought are relevant to an investigation to obtain foreign intelligence information not concerning a USP, **OR**
- Tangible things sought are relevant to an investigation to protect against international terrorism or clandestine intelligence activities

FBI's investigation cannot be conducted of a USP solely upon the basis of activities protected by the First Amendment


(See FISA Titles IV and V)

29

UNCLASSIFIED



UNCLASSIFIED

 OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION

## FISA as amended by the FISA Amendments Act (FAA)

Section 702

Allows for collection against non-US Person reasonably believed to be located outside the US

- Certification by the Attorney General and the Director of National Intelligence, and approved by FISC, and
- Court-approved targeting and minimization procedures

Collection must cease immediately / collection purged if:

- Target is discovered to be a US person
- Target has traveled into the US

Sections 703 and 704

Allows for targeting US Persons overseas with approval of FISC


30

UNCLASSIFIED

### **FISA Amendments 2007 and 2008**

- Made provisions for modernization and minimization
  - Modernization - addressed changes in technology
    - Allows collection against non-USP targets located outside of the U.S. through interception of communications that transit the U.S.
  - Minimization – Procedures to protect USP information
  - Requires a FISC court approval for intrusive intelligence collection on USP overseas
  - Requires a *FISA* caveat for all products that use intelligence derived from *FISA* collection (with the exception of 704/705b collection and Business Records)

UNCLASSIFIED



**OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**  
LEADING INTELLIGENCE INTEGRATION

## FISA as amended by FAA (cont'd)

- FISA /FAA Requires Minimization Procedures
  - Procedures to minimize the acquisition, retention and dissemination of non-publicly available information concerning US Persons, consistent with the need to obtain, produce and disseminate foreign intelligence information (sometimes called Standard Minimization Procedures–SMPs)
- *FISA* caveat prohibits use of products in certain proceedings without advance approval by the Attorney General
- Information collected under FISA/FAA will be governed by FISA/FAA procedures and Court orders
  - FISA/FAA minimization procedures should not be confused with the AG-approved guidelines under EO 12333 for collection, retention, or dissemination of US Person information
  - FISA definitions of foreign intelligence and US person are somewhat different from EO 12333

31


UNCLASSIFIED

FISA caveat typically provides notice that AG approval must be obtained before using FISA derived information in a “criminal proceeding” (that the term has a broad meaning to include for example deportation hearings); agency SMPs vary

Note: there is no caveat required for information obtained under FISA 704/705b and Business Records.

Note: certain SMP procedures also apply to information about non-USPs

UNCLASSIFIED



**OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**  
LEADING INTELLIGENCE INTEGRATION

## The Privacy Act

Provides “individuals” certain rights and assurances, and imposes on the government certain obligations, when federal agencies collect, maintain, and use “records” about those individuals.

- Individual: US citizen or permanent resident alien (different from EO 12333 “US 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)

Applies when the agency routinely retrieves records from a “System of Records” by the individual's name or unique identifier.


- 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

32

UNCLASSIFIED

Because the Privacy Act is a “withholding” statute (it protects against release of information about an individual without his/her consent), it uses the term “share” or “disclose” instead of “disseminate” as used in the IC.

UNCLASSIFIED



**OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**  
LEADING INTELLIGENCE INTEGRATION


## The Privacy Act -- Essentials

- **Systems of Records Notice (“SORN”):** Agencies must publish a SORN in the Federal Register, describing the compilation of records and purpose for the collection
- **Privacy Act Statement/Notice of Collection:** Agencies collecting information directly from an individual must provide notice of the purpose of the collection and the manner in which the agency will use the information
- **Minimum necessary:** Agencies may collect only that information about individuals that is “relevant and necessary” to accomplish an authorized agency purpose
- **First Amendment protection:** Agencies may not collect information about an individual’s First Amendment practices absent authorized law enforcement activity

33

UNCLASSIFIED

UNCLASSIFIED



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION

## The Privacy Act -- Essentials (cont'd)


- **No disclosure without consent:** Agencies may disclose records to outside parties only with the consent of the individual to whom the records pertain, or pursuant to 12 statutorily authorized conditions, including the agency's published "routine uses"
  - **Routine use:** a published determination of the circumstances under which the agency may disclose records outside the agency absent consent if the reason for disclosure is compatible with the purpose for collecting the record
- **Access and amendment:** Subject to exceptions for national security and other prescribed grounds, individuals are entitled to review and correct records that the agency maintains about them

34

UNCLASSIFIED

UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION




## The Privacy Act -- Essentials (cont'd)

- **Data quality:** Agencies must make reasonable efforts to ensure records are as timely, relevant, accurate and complete as necessary for the purpose for which they were collected
  
- **Safeguards:** Agencies must establish appropriate technical and administrative safeguards to ensure the security, confidentiality, integrity and continued availability of records about individuals
  
- **Penalties:** There are civil penalties for agency violations of administrative and technical requirements; also criminal penalties against any officer or employee of an agency who knowingly and willfully disregards notice requirements or prohibitions on disclosure

35

UNCLASSIFIED

UNCLASSIFIED



**OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**  
LEADING INTELLIGENCE INTEGRATION

## Personally Identifiable Information

OMB Memorandum M-07-16:

- The term "personally identifiable information" (PII) refers to information that can be used to distinguish or trace an individual's identity, such as his or her name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

In other words: PII is any data about an individual that actually identifies the individual or may identify the individual when compared or associated with other data.


- A name, SSN, fingerprint or other biometric data are themselves identifiers.
- Street address, telephone number or any other biographic or descriptive data elements are potentially identifying if combined with other data.
  - Example: vehicle identifier (VIN) or license plate numbers; internet protocol addresses; and education, financial or medical information

36

UNCLASSIFIED



UNCLASSIFIED



**OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**  
LEADING INTELLIGENCE INTEGRATION

## Personally Identifiable Information (cont'd)

OMB Memorandum M-10-22:


- The definition of PII is not anchored to any single category of information or technology. Rather, it demands a case-by case assessment of the specific risk that an individual can be identified.
  - Some PII is more sensitive than other PII. "Sensitive PII" is the kind of personal data that, if compromised, could cause practical harm:
    - economic
    - reputational
    - physical
- Even though many collections of records are not Privacy Act Systems of Records (because they are not retrieved by a unique personal identifier), if they contain PII, they must be protected.

37

UNCLASSIFIED

Note re sensitive PII: for example, a bank account number combined with a name is more sensitive than a place of birth combined with a name, because disclosure of this bank account/name information could result in identity theft, fraud, misappropriation of personal assets. The bank account and name combination might therefore be considered "sensitive PII."

UNCLASSIFIED



**OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**  
LEADING INTELLIGENCE INTEGRATION


## PII Protections/OMB Requirements

- OMB Memorandum 06-15, Safeguarding Personally Identifiable Information (May 22, 2006)
  - 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 Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007)
  - Directs agencies to establish incident response procedures to assess and mitigate the potential harm to individuals arising from unauthorized use or disclosure of PII
  - An IC professional who learns of an unauthorized disclosure of PII should immediately report such disclosure to appropriate officials at the element so that privacy risk analyses and proper steps can be taken

38

UNCLASSIFIED

UNCLASSIFIED



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION


## The Information Sharing Environment (ISE)

- Defined in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Section 1016, as “an approach that facilitates the sharing of terrorism information.”
  
- Section 1016 charges the President to:
  - Create a terrorism information sharing framework that honors applicable legal standards relating to privacy and civil liberties
  
  - Vision: a **trusted partnership** at all levels of government in the US, the private sector, and our foreign partners

39

UNCLASSIFIED

UNCLASSIFIED



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION

## The Information Sharing Environment (ISE) Privacy Guidelines


- Implement the requirements of the IRTPA and Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans*
  - Create a common framework to ensure Federal agencies implement the core privacy protections in a consistent manner:
    - Core protections: redress; notice mechanisms; data quality; data security; and accountability, enforcement, and audit
  - Designed to protect information privacy and civil liberties based on rules and agency mission
  - As implemented, includes requirement for written, agency-specific, ISE Privacy and Civil Liberties policies

40

UNCLASSIFIED

UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION



## Other Laws

- Apply to certain systems, activities and data, such as:
  - E-Government Act
  - Freedom of Information Act
  - Data Mining Reporting Act
  - Electronic Communications Privacy Act
  - Stored Communications Act
  - Right to Financial Privacy Act
  - Health Insurance Portability and Accountability Act
  - Etc.

41

UNCLASSIFIED

Notes re E-Government Act (section 208):

Mandates Privacy Impact Assessment (PIA) for non-national security-systems (NSS) as defined by statute


- PIA is an assessment of the risks to privacy and civil liberties arising from an electronic business process involving PII, and an evaluation of the sufficiency of privacy and civil liberties safeguards and measures applied.
- (PIA considers: type of information; why

collected; how used/shared/secured; whether Privacy Act applies; whether collected/used with subjects' consent; risks to privacy/civil liberties; if/how risks are mitigated by policy or technical fixes.)

Establishes criteria for evaluating the privacy implications of IT systems projects, and new electronic collections of PII:

- Notwithstanding the exemption for NSS, many elements formally or informally consider the privacy implications for all information systems and electronic collections that use or collect PII

UNCLASSIFIED



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION

## Course Summary

- There are numerous rules to understand and consider when dealing with information concerning protected individuals and entities
- Remember that the requirements of EO 12333 alone do not govern the collection, retention, or dissemination of information about US persons; an IC element's collection and use of US person information **must** accord with that element's mission and with its AG- approved guidelines/procedures
- When applying statutory and regulatory requirements for protecting privacy and civil liberties, work with in-house experts (Offices of General Counsel and Privacy /Civil Liberties /Civil Rights Officials) to understand how these requirements may impact your activities
- This module is foundational, to be supplemented by in-depth training tailored to each IC element's mission and specific training needs


42

UNCLASSIFIED

- Each organization's procedures are **unique** - one size does **not** fit all
- **But** underlying principles **are applicable to all**



UNCLASSIFIED



OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE  
LEADING INTELLIGENCE INTEGRATION

**Questions?**

43

UNCLASSIFIED