

UNCLASSIFIED



SAFEGUARDING PERSONAL INFORMATION

NATIONAL ARCHIVE RECORDS SERVICE

PA101: Privacy Act Safeguarding Personal Information



UNCLASSIFIED



SAFEGUARDING PERSONAL INFORMATION

INTEL 1001 COURSE ID: INTEL1001

[MENU](#) [GLOSSARY](#) [RESOURCES](#)

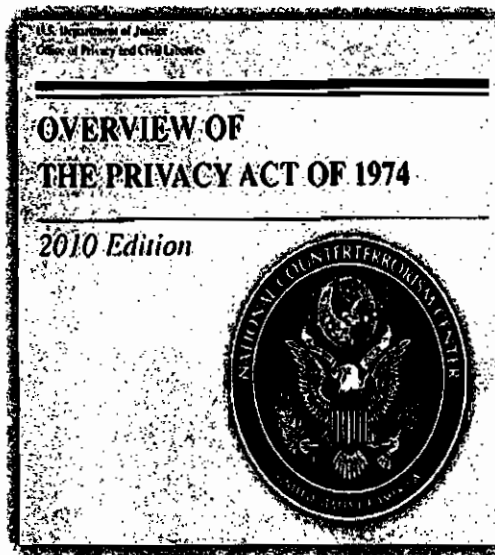
Introduction and Overview

To conduct its business, the Federal Government, including the Intelligence Community (IC), collects, maintains and discloses information about American citizens and permanent resident aliens.

In 1974, the Privacy Act was established to protect these individuals' rights with regard to how the government uses the information it collects about them.

Upon completing this course, you will be able to:

- Describe how the Privacy Act of 1974 protects individuals' rights regarding information collected, maintained and disclosed about them by the Federal Government
- Define Personally Identifiable Information (PII) and how it is protected



[How to Take This Course](#)



Web Accessibility

10

How to Take This Course

For more information on how to take this course, please visit the course page.

For more information on how to take this course, please visit the course page.

How to Take This Course

Screen Resolution

The course is designed to be viewed on a screen with a resolution of 1024x768 pixels. If you are viewing the course on a screen with a different resolution, the content may not display correctly.

Navigation

The course is designed to be viewed on a screen with a resolution of 1024x768 pixels. If you are viewing the course on a screen with a different resolution, the content may not display correctly.

Resources

For more information on how to take this course, please visit the course page.

Assessment

The course is designed to be viewed on a screen with a resolution of 1024x768 pixels. If you are viewing the course on a screen with a different resolution, the content may not display correctly.

CLOSE

UNCLASIFIED

UNCLASIFIED

UNCLASSIFIED



SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERINTELLIGENCE CENTER

[MENU](#) : [GLOSSARY](#) : [RESOURCES](#)

Module Selection

Select a link to begin.

[Lesson 1: Overview of Privacy](#)[Lesson 2: What is the CIA doing with](#)[Lesson 3: What is CIA](#)[Lesson 4: Privacy and Information Security](#)[How to Take This Course](#)

UNCLASSIFIED

UNCLASSIFIED

Glossary/Acronym List

Roll over underlined terms to view a definition of the term.

AG = Attorney General

CLPO = Civil Liberties and Privacy Office

CT = Counterterrorism

DMT = Data Management Team

EO = Executive Order

FISA = Foreign Intelligence Surveillance Act

FOIA = Freedom of Information Act

HHS = Department of Health and Human Services

IC = Intelligence Community

ISE = Information Sharing Environment

ISSM = Information Systems Security Manager

NCTC = National Counterterrorism Center

NCTC/ISPPD = National Counterterrorism Center/Information Sharing Program Policy Office

PA = Privacy Act

PII = Personally Identifiable Information

SORN = System of Records Notice

SSC = Special Security Center

SSN = Social Security Number

TI = Terrorism Information

USP = United States person

CLOSE

UNCLASSIFIED

UNCLASSIFIED

Take Privacy Act Disclosures

Sample NCYC CORN

ODM Routine Users

Sample Privacy Act Statement

EO 12812

Privacy Act of 1974

CLOSE

UNCLASSIFIED



SAFEGUARDING PERSONAL INFORMATION

NATIONAL INFORMATION SECURITY ADMINISTRATION

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)

Introduction and Objectives

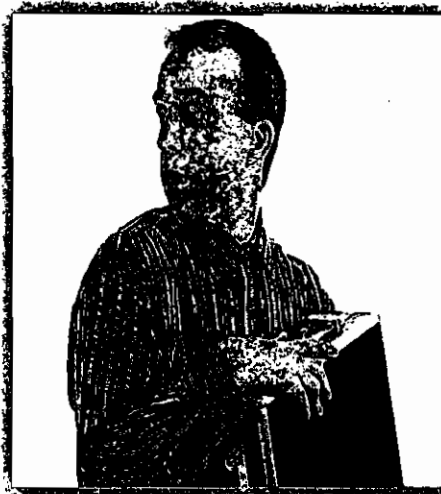
The word "privacy" is not used anywhere in the Constitution. However, the Constitution has been interpreted by the courts to provide several constitutionally protected rights that reflect privacy-related interests (for example the Fourth Amendment's right to be secure in our homes and possessions).

There are many facets to privacy. Here, we will consider privacy to be the ability to control what the government knows about us.

In addition to the Constitutional protections of privacy, there are many different laws that protect the "privacy" of citizens or other members of the public. This lesson addresses protections for individuals' "information privacy." Specifically, we will discuss limitations on the Federal Government's collection and handling of information from or about individuals.

Upon completing this lesson, you will be able to:

- Identify the principal authorities that IC professionals should be familiar with relating to information privacy



LESSON TITLE: Overview of Privacy





SAFEGUARDING PERSONAL INFORMATION

NATIONAL SECURITY AGENCY INFORMATION CENTER

[MENU](#) [GLOSSARY](#) [RESOURCES](#)

Principal Authorities

As stewards of data, you need to be aware of the principal legal and Executive-level protections for information privacy that govern our actions as federal employees. Two of the primary sources of these obligations are:

- The Privacy Act of 1974
- Executive Order (EO) 12333 (covered in separate training)

Click on each document for additional details on protection of information.

The Privacy Act

EO 12333

Executive Order 12333
Protection of Information

LESSON TITLE: Overview of Privacy



UNCLASSIFIED

CONFIDENTIALITY OF INFORMATION

CONFIDENTIAL

CONFIDENTIAL

CONFIDENTIALITY OF INFORMATION
CONFIDENTIALITY OF INFORMATION
CONFIDENTIALITY OF INFORMATION

CONFIDENTIALITY OF INFORMATION

CLOSE

UNCLASSIFIED

UNCLASSIFIED

SAFETY INFORMATION PERSONAL INFORMATION

PERSONAL INFORMATION PERSONAL INFORMATION

PERSONAL INFORMATION PERSONAL INFORMATION

EO 12958 defines U.S. Persons (USP) and provides guidance on collecting, retaining, and disseminating USP information. For EO 12958, a USP is a U.S. citizen, an alien born in the United States, an alien born in a permanent resident status, an unincorporated corporation substantially composed of U.S. citizens or permanent resident alien, or a corporation incorporated in the U.S. except for corporations created and controlled by a foreign government or governments.

A person who is not a USP is not a USP.

CLOSE

UNCLASSIFIED



SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERINTELLIGENCE CENTER

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)

Why Is Information Privacy Important?

Complying with information privacy protections fosters trust from the public, our mission partners and other stakeholders that we are properly using and protecting the data that 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.



LESSON TITLE: Overview of Privacy



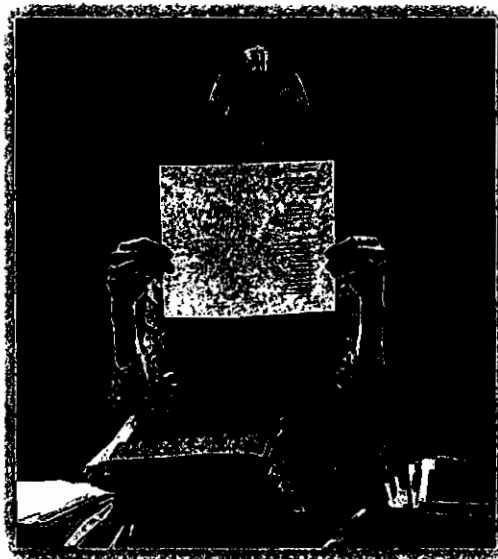
**SAFEGUARDING PERSONAL INFORMATION**

NATIONAL CHILD PROTECTION CENTER

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)**Summary**

You have completed the lesson, Overview of Privacy. In this lesson, you were introduced to the principal legal and Executive-level authorities regarding the protection of information about U.S. Persons (USP).

The next lesson explores The Privacy Act of 1974 in detail.

**LESSON TITLE:** Overview of Privacy



SAFEGUARDING PERSONAL INFORMATION

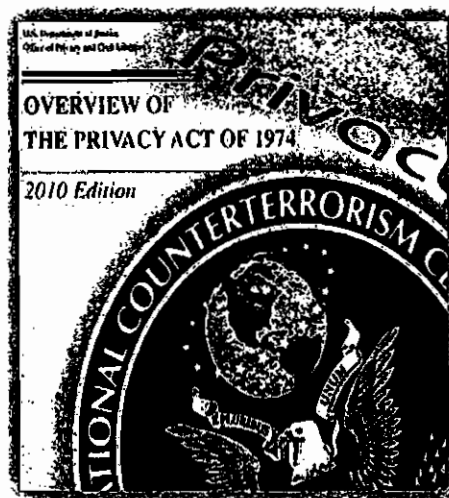
NATIONAL COUNTERTERRORISM CENTER

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)**Introduction & Overview**

The Privacy Act of 1974 provides the Federal Government with rules for collecting and handling information about individuals (defined by the Act as U.S. citizens and legal permanent residents). In addition, the Privacy Act affords these individuals certain rights, which are designed to protect their privacy and hold the government accountable for how it uses their data.

Upon completing this lesson, you will be able to:

- Identify the purpose of the Privacy Act
- Identify when the Privacy Act applies
- Describe the protections the Privacy Act affords individuals

**LESSON TITLE:** What is the Privacy Act?



SAFEGUARDING PERSONAL INFORMATION

UNIT 1: LESSON 1: SAFEGUARDING PERSONAL INFORMATION

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)**The Privacy Act**

Prior to enactment of the Privacy Act in 1974, there were instances when some law enforcement and intelligence agencies inappropriately collected and used information about U.S. citizens.

The purpose of the Privacy Act is to:

- Protect against illegal secret collection of records by the government
- Govern collection, maintenance and disclosure of information about individuals
 - The Privacy Act does not apply to statistical or aggregate information where the individual cannot be identified, such as census data or data collected for a statistical analysis
- Provide substantive rights to individuals

LESSON TITLE: What is the Privacy Act?





SAFEGUARDING PERSONAL INFORMATION

NATIONAL COMPUTER FORENSIC CENTER

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)

Who Is Protected?

The Privacy Act provides protection to an "individual," who is defined as a:

- Living human being (not deceased)
- U.S. citizen or permanent resident alien
 - NOTE: Be alert to situations when an "individual" may also be acting as a business (e.g., Alex Accountant runs Alex Accountant LLC). In those situations contact NCTC Legal for further guidance.

Compare this definition of an "individual" under the Privacy Act with the definition of a "U.S. Person" under EO 12333, who is defined as a:

- U.S. citizen or permanent resident alien,
- Unincorporated association substantially composed of U.S. citizens or permanent resident aliens, or
- Corporation incorporated in the U.S. except for a corporation directed and controlled by a foreign government or governments

LESSON TITLE: What is the Privacy Act?





SAFEGUARDING PERSONAL INFORMATION

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

MENU | GLOSSARY | RESOURCES

When Does the Privacy Act Apply?

The requirements of the Privacy Act apply whenever agencies collect, maintain and administer records about an individual, and the agency retrieves those records by the individual's name or other unique personal identifier, such as:

- A Social Security Number (SSN)
- An employee ID number
- Finger prints
- A voice print
- A photograph of the individual

Example: If Agency A maintains a database of U.S. Passport holders and retrieves those records by an individual's name or SSN, the Privacy Act applies. If Agency A maintains a database of U.S. Passport holders, but only retrieves those records by the passport center where the passport was issued, the Privacy Act would not apply because the city of passport issuance is not a unique personal identifier.



LESSON TITLE: What is the Privacy Act?





SAFEGUARDING PERSONAL INFORMATION

NATIONAL CIVIL LIBERTIES UNION

MENU | GLOSSARY | RESOURCES

What is a System of Records Notice?

You have learned that the Privacy Act applies when a government agency collects information from, or about, individuals and then retrieves those records by the individual's name or other unique personal identifier.

This cumulative collection of records is known as a Privacy Act "System of Records." Because a primary goal of the Privacy Act is to inform individuals about how the government uses their information, the Privacy Act requires Federal agencies to provide public notice about how they administer these "Systems of Records." Notice is provided through a "System of Records Notice" or "SORN" that is published in the Federal Register. The SORN describes the existence, type (e.g., whether medical, personnel, financial, etc.) and purpose of the records, and the "routine uses" for which information from the record can be shared external to the agency without the consent of the individual.

Select the link to view a sample NCTC [SORN](#).

LESSON TITLE: What is the Privacy Act?





SAFEGUARDING PERSONAL INFORMATION

NATIONAL SECURITY AGENCY

MENU | GLOSSARY | RESOURCES

Collection of Records

Under the Privacy Act, agencies must follow these guidelines when collecting information about individuals.*

- Collect the information directly from the individual, when feasible.
- Provide individuals with a "Privacy Act Statement" at the time of collection (i.e., notice of the legal authority under which the government is collecting the information and how the government intends to use that information).
- Collect only the minimum amount of information necessary to accomplish the agency's purpose.

**There are exemptions from these requirements when records are collected for authorized investigatory and national security purposes. If an agency uses an exemption, that exemption is referenced in the published SORN for the records to which the exemption applies.*

Select the link to view a sample [Privacy Act Statement](#)



COLLECTION



MAINTENANCE



ACCESS



DISCLOSURE

LESSON TITLE: What is the Privacy Act?





SAFEGUARDING PERSONAL INFORMATION

NATIONAL INSTITUTE OF JUSTICE TRAINING CENTER

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)

Maintenance of Records

When maintaining records about individuals under the Privacy Act, agencies generally must:

- Keep timely, relevant, accurate and complete records
- Permit record subjects to:
 - Access records
 - Amend records
 - Obtain information about when and to whom his or her records have been disclosed
- Keep no records that are based solely upon the exercise of First Amendment rights

NOTE: There are exemptions from these requirements when records are maintained for authorized investigatory and national security purposes.



COLLECTION



MAINTENANCE



ACCESS



DISCLOSURE

LESSON TITLE: What is the Privacy Act?





SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERTERRORISM CENTER

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)

Individuals' Access to Records

The Privacy Act dictates that agencies must establish procedures for individuals to follow to gain access to their records. In general, individuals have the right of access to records about themselves. However, if records have been collected for an investigatory or national security purpose, the government agency may be exempt from the requirement of providing the individual with access to his or her records (so as not to "tip" the subject about the investigatory or national security interest). The SORN provides public notice about whether the agency has invoked any such exemptions.

For additional information about how or whether individuals can gain access to records about themselves, consult NCTC Legal or the NCTC Civil Liberties and Privacy Office (CLPO).



COLLECTION



MAINTENANCE



ACCESS



DISCLOSURE

LESSON TITLE: What is the Privacy Act?





SAFEGUARDING PERSONAL INFORMATION

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

[MENU](#) [GLOSSARY](#) [RESOURCES](#)

Disclosure or Dissemination of Records

Agencies may only disclose or disseminate Privacy Act records (maintained in a System of Records) outside the agency in the following circumstances:

- With the consent of the record subject.
- For the twelve exempted disclosures authorized in subsection (b) of the Privacy Act. These twelve disclosures are exceptions to the "consent rule" (above) and generally permit disclosures to named agencies or government entities for purposes limited to execution of their statutory responsibilities (e.g., disclosure of records to the National Archives and Records Administration for audit of compliance with records management requirements).
- When permitted by a published "routine use". A "routine use" is an explanation of how the agency regularly shares data it maintains in a Privacy Act System of Records with entities outside the agency. The agency provides notice of these "routine uses" when it publishes its SORN. An example routine use might entail disclosure to the Department of Justice of information relating to ongoing litigation.

Select the link for a sample of routine uses from the [ODNI Privacy Act Regulation](#).



COLLECTION



MAINTENANCE



ACCESS



DISCLOSURE

LESSON TITLE: What is the Privacy Act?





SAFEGUARDING PERSONAL INFORMATION

NATIONAL INFORMATION SECURITY COUNCIL

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)

Sanctions for Violating the Privacy Act

Violations of the Privacy Act can result in personal liability and actions against the agency:

- Agency employees can be subject to criminal penalties or agency administrative actions for inappropriate disclosures of Privacy Act protected information
- Agencies themselves may be subject to civil action in Federal court for non-compliance with the Privacy Act



LESSON TITLE: What is the Privacy Act?





SAFEGUARDING PERSONAL INFORMATION

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

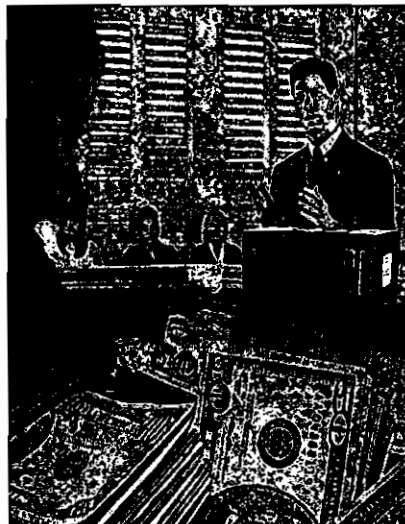
MENU | GLOSSARY | RESOURCES

Penalties and Results

Employees can be charged with a misdemeanor, subject to a \$5,000 fine if they:

- Willfully disclose Privacy Act protected material by any means to any person or agency not entitled to receive it
- Willfully maintain a System of Records without meeting the SORN publication requirement
- Willfully request or obtain any record concerning an individual from an agency under false pretenses

Agencies may be prohibited from using and sharing records compiled in a System of Records if they do not publish a SORN.



LESSON TITLE: What is the Privacy Act?





SAFEGUARDING PERSONAL INFORMATION

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)**Summary**

You have completed the lesson, What is the Privacy Act? The Privacy Act protects against illegal secret collection of information by the government; governs collection, maintenance and disclosure or dissemination of that information; and affords substantive rights (notice, consent, access and legal right of action) to the individuals about whom the information is collected, maintained and administered. It also prescribes penalties for violating these protections.

The next lesson will look at Personally Identifiable Information (PII) in more detail.

LESSON TITLE: What is the Privacy Act?



SAFEGUARDING PERSONAL INFORMATION

FEDERAL BUREAU OF INVESTIGATION

MENU | GLOSSARY | RESOURCES

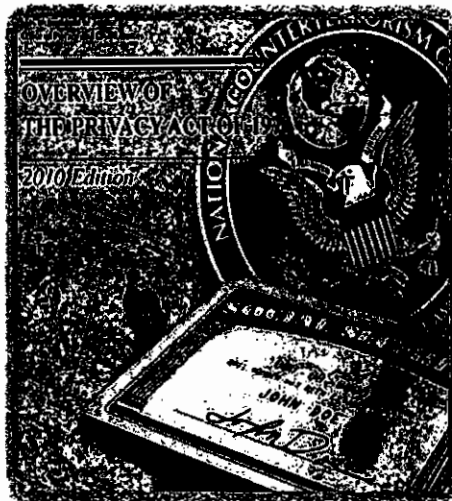
Introduction and Overview

Technology enables Federal agencies to maintain a great deal of information about individuals. The collection and consolidation of this information by the government is a legitimate privacy concern for Americans, and we have a special duty to protect such information from loss and misuse.

It is your responsibility to understand the sensitivity of personal information and the rules that govern its collection and use.

Upon completing this lesson, you will be able to:

- Identify protection for Personally Identifiable Information (PII)
- List expectations for handling PII



LESSON TITLE: What is PII?



SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERINTELLIGENCE CENTER

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)

What is Personally Identifiable Information (PII)?

The term PII is defined in OMB Memorandum M-07-16 as:

"...information which can be used to distinguish or trace an individual's identity, such as their 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, place of birth, mother's maiden name, etc."

In essence, PII is any biographic or descriptive data that, alone or in combination with other data, can identify an individual either directly (by name) or indirectly (i.e., can be used to figure out the identity of the person being described).

Because Privacy Act records - by definition - are retrieved by unique personal identifiers, all Privacy Act Systems of Records contain PII.

LESSON TITLE: What is PII?





SAFEGUARDING PERSONAL INFORMATION

NATIONAL CYBERSECURITY CENTER

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)

Sensitive PII

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

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 or name information could result in:

- Identity theft
- Fraud
- Misappropriation of personal assets

The bank account and name combination might therefore be considered "sensitive PII."



LESSON TITLE: What is PII?





SAFEGUARDING PERSONAL INFORMATION

NATIONAL INTELLIGENCE COMMUNITY

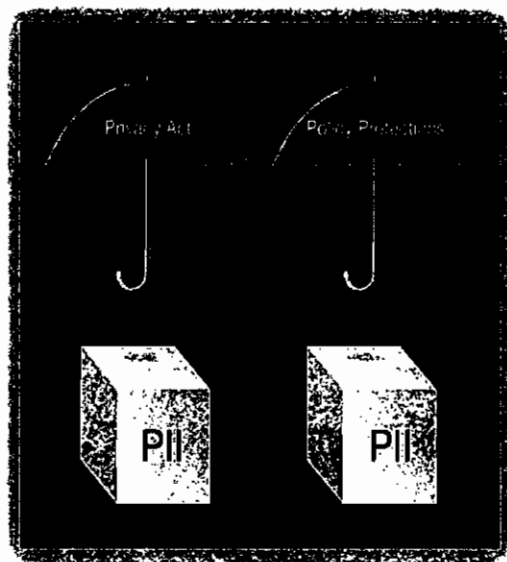
MENU | GLOSSARY | RESOURCES

PII versus Privacy Act-Protected Records

Even though some collections of records are not Privacy Act Systems of Records (i.e., because they are not retrieved by a unique personal identifier), they may still contain PII. To the extent that these collections of records contain PII, they must be protected.

Example: Consider a database with the names of IC analysts, their education and credentials. The database is queried by area of expertise, such as "China analysts" or "cyber security specialists." Because the query retrieves information by area of expertise, and not by unique personal identifier, the returned information was not maintained in a System of Records and thus is not covered by the Privacy Act. Nonetheless, because the returned information does contain analysts' names and related biographical information - which is PII - we must protect this PII accordingly.

So, Privacy Act records contain PII, but not all records containing PII are protected by the Privacy Act.



LESSON TITLE: What is PII?



UNCLASSIFIED



SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNCIL ON CYBER SECURITY

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)**How Should PII be Protected?**

Various OMB Policy Memoranda require federal agencies to ensure the protection of PII through appropriate administrative, technical and physical safeguards.

These safeguards limit records access to only those who have an authorized purpose. They also protect against threats or hazards to the security or integrity of the PII, which could result in harm, embarrassment, inconvenience or unfairness to any individual about whom the information pertains.

Many IC personnel mistakenly believe that the classified environment in which we work is, in itself, protective of PII. Not necessarily so. For example, even in a secure environment, it is improper to leave a spreadsheet of names with SSNs or medical information open to general view (e.g., leaving a paper containing SSNs on a conference room table viewable by all attendees).

As a practical matter, many of our internal security procedures for handling sensitive information already afford protection for PII.

NOTE: Any time that an employee creates or downloads extracts from databases holding sensitive PII, the employee will need to ensure that this PII is tracked and properly protected. For more specific guidance on protections, contact NCTC Legal or NCTC CLPO.

LESSON TITLE: What is PII?



UNCLASSIFIED



SAFEGUARDING PERSONAL INFORMATION

NATIONAL OFFICE OF INFORMATION SECURITY

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)**Reporting Breaches of PII**

In order to prevent the harms that can potentially result from unauthorized disclosure of PII or sensitive PII, it is important that actual or suspected breaches or compromises of data about individuals be reported to the ODNI CLPO, per ODNI Instruction 80.02, *Managing Breaches of Personally Identifiable Information*.

- Individuals who fail to safeguard PII as required by law, regulation or policy - or fail to report known or suspected loss of control or unauthorized disclosure of PII - may be subject to disciplinary action, regardless of whether the failure results in criminal prosecution, civil penalties, or sanctions under applicable law.

Upon receipt of a report of actual or suspected breach, the ODNI CLPO will convene an incident response team to investigate the circumstances.

NOTE: Other mandatory ODNI reporting requirements may apply (e.g., reporting computer security events and incidents to ODNI Information Systems Security Manager (ISSM), reporting unauthorized disclosures of classified information to ODNI Special Security Center (SSC), etc.).

LESSON TITLE: What is PII?





SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERTERRORISM PROGRAM CENTER

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)**What is the Information Sharing Environment (ISE)?**

The Information Sharing Environment (ISE) is a framework created for sharing and integrating terrorism information between different levels of government, the private sector and foreign partners in a manner that protects privacy rights, civil liberties and other legal rights of individuals.

- Creature of the IIRTPA (section 1016), conceived to help "connect the dots"
- Builds on Executive Order 13388, which requires agencies possessing/acquiring terrorism information to provide that information to other agencies with authorized counterterrorism functions

The ISE is NOT a single database, system or repository! It is a framework of policies, procedures and technology.

LESSON TITLE: What is PII?





SAFEGUARDING PERSONAL INFORMATION

NATIONAL INFORMATION SECURITY AGENCY

MENU | GLOSSARY | RESOURCES

What are the ISE Privacy Guidelines?

- Presidentially-mandated Guidelines that establish a core set of principles that ensure consistent vetting of "protected information" within the ISE through the adoption of best practices designed to protect individuals' information privacy and civil liberties.
- Protected information includes USP information, but *may also* be broader. According to the Privacy Guidelines, information may be designated as subject to ISE information privacy protections by Executive Order, international agreement or other legal instrument.
- Some of the core privacy and civil liberties protections include: procedures to prevent, identify and correct errors in shared information; measures to safeguard ISE information; procedures for receiving and addressing complaints related to the sharing of protected information; and procedures for reviewing/verifying compliance with the agency ISE policy and responding to violations.
- The Guidelines require all entities that participate in the ISE to develop an information handling policy consistent with the Guidelines.
- The ODNI's implementing policy is ODNI ISE Privacy Instruction - 80.05 (September 2009)

LESSON TITLE: What is ISE?





SAFEGUARDING PERSONAL INFORMATION

NATIONAL INTELLIGENCE INFORMATION

MENU | GLOSSARY | RESOURCES

What does the ISE mean to you?

- NCTC is a part of the ISE and operates under ODNI Privacy Instruction 80.05
- The core ISE protections that most directly affect your work include ensuring:
 - information you receive/disseminate has some indication of reliability (or lack thereof)
 - that data you handle is reliable and up to date, to the extent feasible
 - familiarity with the NCTC process for correcting errors (whether the error was discovered by you, or by the agency that provided you the data)
 - appropriate handling and protection of personally identifying information (PII) in the data.
- If you have additional questions on the ISE, you can contact NCTC CLPO at LN Group Alias

LESSON TITLE: What is PII?



SAFEGUARDING PERSONAL INFORMATION

INSTITUTIONAL AND COMMUNITY RELATIONS DIVISION

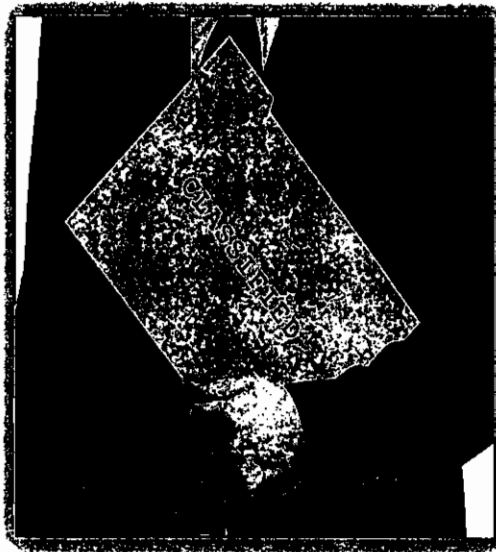
[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)

Summary

You have completed the lesson. What is Personally Identifiable Information. In this lesson you have learned to recognize PII and sensitive PII and to appreciate the ramifications of unauthorized disclosure of PII.

You can now identify some of the technical, administrative, and physical safeguards that agencies implement to protect PII, and understand the importance of reporting spills of PII.

The next lesson will cover the requirements and limitations of the Privacy Act.



LESSON TITLE: What is PII?





SAFEGUARDING PERSONAL INFORMATION

NATIONAL CIVIL LIBERTIES PROGRAM CENTER

MENU | GLOSSARY | RESOURCES

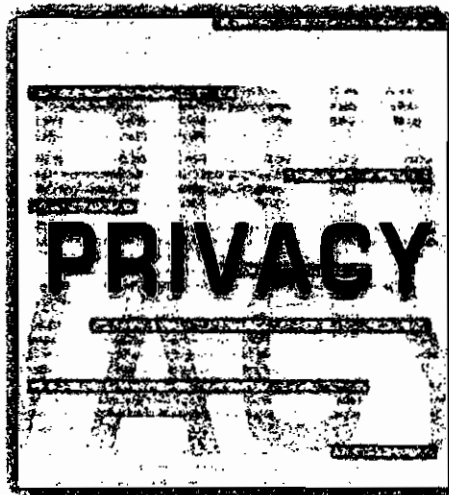
Introduction and Overview

As you have learned, the Privacy Act establishes requirements and prohibitions that agencies must honor when collecting, maintaining and disclosing or disseminating information about individuals.

All NCTC employees must be familiar with these requirements and prohibitions, so as not to violate the Act inadvertently.

Upon completing this lesson, you will be able to:

- Identify those requirements or prohibitions of the Privacy Act that may apply to you personally as you perform your day-to-day duties and responsibilities



LESSON TITLE: Privacy Act Requirements and Limitations





SAFEGUARDING PERSONAL INFORMATION

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)**Your Responsibilities Under the Privacy Act**

You have several responsibilities under the Privacy Act related to the following:

- Maintenance of records
- Access to records
- Disclosure or dissemination of records
- Integrity of records
- Training

LESSON TITLE: Privacy Act Requirements and Limitations





SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERTERRORISM CENTER

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)**Your Responsibilities Under the Privacy Act - Maintenance of Records**

Maintain only relevant records necessary to accomplish a required agency mission.

- For NCTC, these must relate to the Counterterrorism (CT) mission.

Guard against creating a System of Records for which a SORN has not been published.

Example: If an analyst collects publicly available information about individuals from the Internet and stores the search results by the subject's unique personal identifiers, this may constitute a new System of Records. However, if the analyst compiles a spreadsheet from NCTC's existing data holdings, in order to aid his analysis of the data, this is not likely going to be a new System of Records. Of course, if this data comes from an existing System of Records, the spreadsheet is considered derived from that System of Records and should be protected as Privacy Act information.

NOTE: If you have any questions, please contact NCTC Legal or NCTC CLPO.

Protect all Privacy Act records received.

- Be aware that Privacy Act records received from another agency will either be incorporated into an existing ODNI or NCTC System of Records, or may constitute a new System of Records for which ODNI or NCTC would publish a new SORN.

LESSON TITLE: Privacy Act Requirements and Limitations





SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERTERRORISM CENTER

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)

Your Responsibilities Under the Privacy Act Maintenance of Records (continued)

Watch for records describing First Amendment activities!

- NCTC may not maintain such information unless:
 - A statute permits,
 - The subject individual consents, or
 - An authorized law enforcement or intelligence activity supports collection.
- NCTC should not maintain any record in TIDE (or other NCTC database) regarding an "individual's" exercise of protected activity (e.g., religion, expression, association, etc.), with no apparent basis.
 - For example, collecting the names of individuals solely because they spoke at a rally in support of Iran, vice collecting those names because they were invited to speak by a known TIDE subject.

If you have any concerns, contact NCTC Legal or NCTC CLPO for guidance.



LESSON TITLE: Privacy Act Requirements and Limitations



SAFEGUARDING PERSONAL INFORMATION

NATIONAL DEFENSE INFORMATION CENTER

MENU | GLOSSARY | RESOURCES

Your Responsibilities Under the Privacy Act - Access to Records

Ensure needs-based access by analysts to NCTC records.

- An analyst must have a legitimate need for the record in the performance of his or her duties
- Browsing or other unofficial use of records (e.g., searches based on personal interest or unofficial request of another) is prohibited by NCTC policy. Such conduct might also violate the Privacy Act.

Ensure appropriate access by individuals to records maintained about them.

- ODNI's Privacy Act Regulation describes how individuals may request access to records that pertain to them
- Such requests for access are often submitted as Privacy Act or Freedom of Information Act (FOIA) Requests
- Forward all such requests or inquiries for records to NCTC Legal

LESSON TITLE: Privacy Act Requirements and Limitations



TOP SECRET

UNCLASSIFIED



SAFEGUARDING PERSONAL INFORMATION

NATIONAL CONFIDENTIALITY CENTER

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)

Your Responsibilities Under the Privacy Act - Disclosure or Dissemination of Records

Privacy Act records may be disclosed or disseminated as follows:

- With the consent of the individual record subject
- In accordance with twelve excepted disclosures listed in subsection (b) of the Privacy Act. These twelve disclosures are exceptions to the "consent rule" (above) and generally permit disclosures to named agencies or government entities for purposes limited to execution of their statutory responsibilities (e.g., disclosure of records to the National Archives and Records Administration for audit of compliance with records management requirements).
- In accordance with established ODNI routine uses set forth in Section 1701.31 of the ODNI Privacy Act Regulation

Do not disclose or disseminate, through any means, any information from a Privacy Act System of Records, to any person or entity (including other government entities) without consent, a specific routine use, or a statutory exception. This prohibition on disclosures includes oral, written and electronic disclosures.

- All disclosures or disseminations must be made through official channels using approved methods.
- There is no "National Security" exemption from these limitations on sharing records



LESSON TITLE: Privacy Act Requirements and Limitations



UNCLASSIFIED

SAFEGUARDING PERSONAL INFORMATION

MENU | GLOSSARY | RESOURCES

Your Responsibilities Under the Privacy Act - Data Integrity

Prior to use or dissemination of records maintained in a Privacy Act System of Records, make reasonable efforts to ensure records are as timely, relevant, accurate and complete as possible.

- If you find an error, notify National Counterterrorism Center/Information Sharing Program Policy Office (NCTC/ISPPPO) and the Data Management Team (DMT) immediately. An individual's civil liberties may be infringed if action is taken against them based on inaccurate or incomplete information.

Inter-agency agreements may require notification to the data originator of any identified errors, as well as a change to the record copy.

- Again, bring this to the attention of NCTC/ISPPPO and DMT, who will notify the originators of any errors in the records.



LESSON TITLE: Privacy Act Requirements and Limitations





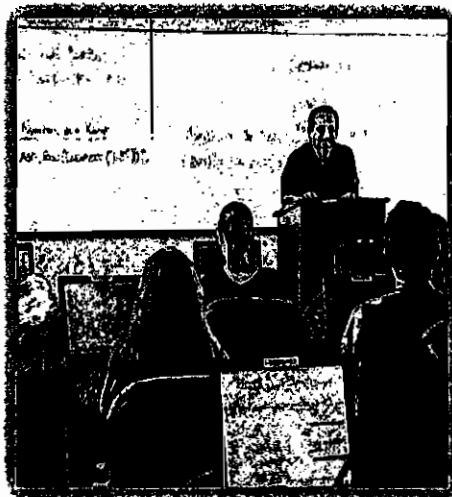
SAFEGUARDING PERSONAL INFORMATION

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)**Your Responsibilities Under the Privacy Act - Training**

The Privacy Act mandates awareness training for all agency personnel, to include cadre employees, detailees, assignees and contractors.

Depending on your particular responsibilities, you may receive additional training on specific administrative, technical and physical safeguards to ensure the security and confidentiality of records.



LESSON TITLE: Privacy Act Requirements and Limitations





SAFEGUARDING PERSONAL INFORMATION

LESSON 1: PRIVACY ACT REQUIREMENTS AND LIMITATIONS

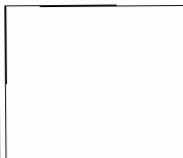
[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)

Summary

You have now completed the lesson, Privacy Act Requirements and Limitations. You must be familiar with all requirements and prohibitions established under the Privacy Act regarding:

- Maintenance of records
- Access to records
- Disclosure or dissemination of records
- Integrity of records
- Training

For additional information, please send a request using the following Lotus Notes aliases:



LESSON TITLE: Privacy Act Requirements and Limitations





SAFEGUARDING PERSONAL INFORMATION

THE NATIONAL COUNTERTERRORISM CENTER

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)

Safeguarding Personal Information Course Summary

You have now completed the course, NCTC Privacy ACT 101: Safeguarding Personal Information. The Privacy Act of 1974 protects information maintained in a Privacy Act System of Records and individuals' rights regarding that information. Various regulations and policy issuances prescribe safeguards for other personally identifiable information.

Note that the Privacy Act provides a basic framework. Some agencies go beyond this framework to extend protections to persons not covered by the Act (e.g., foreign nationals) or to prescribe information safeguards not contemplated by the Act. When an inter-agency sharing agreement reflects additional protections specified by the sharing agency, NCTC will honor the terms of the agreement, provided they are not inconsistent with the Privacy Act.

Today's training complements other training you have (or will receive) regarding the protection of information relating to American citizens and other U.S. Persons (USP). Additional modules relate to USP rules under EO 12333; Foreign Intelligence Surveillance Act (FISA); NCTC Attorney General (AG) Guidelines; Information Sharing Environment (ISE) Privacy Guidelines, and others.

Click NEXT to complete the course post test.

LESSON TITLE: Privacy Act Requirements and Limitations





SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERTERRORISM CENTER

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)

Question 1 of 10

Which of the following provision(s) do NOT govern the Federal Government's activity relating to information about U.S. citizens?
Select the best response and select SUBMIT.

- ☐ A. The Privacy Act of 1974
- ☐ B. Executive Order (EO) 12333
- ☐ C. The Federal Information Security Management Act (FISMA)

SUBMIT

LESSON TITLE: Post Test



SAFEGUARDING PERSONAL INFORMATION

NEW FROM THE OFFICE OF PERSONAL IDENTITY PROTECTION

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)

Question 2 of 10

Which of the following is considered an "individual" protected by the Privacy Act?
Select the best response and select SUBMIT.

- ☐ A. A U.S. born citizen who recently passed away at the age of 93
- ☐ B. A U.S. Corporation incorporated in the State of Delaware
- ☐ C. A refugee from Burma (Myanmar) who just received his citizenship
- ☐ D. The newly formed U.S.-based not-for-profit group, "People For a Better Yesterday"

SUBMIT

LESSON TITLE: Post Test



SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERINTELLIGENCE CENTER

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)

Question 3 of 10

Which of the following is NOT a purpose of the Privacy Act?
Select the best response and select SUBMIT.

- ☐ A. To protect against secret collection of records by the Federal Government
- ☐ B. To govern the Federal Government's collection, maintenance and disclosure of information from or about identifiable individuals
- ☐ C. To provide substantive rights to individuals regarding access to, and correction of, records held about them by the Federal Government
- ☐ D. To protect against online identity theft

SUBMIT

LESSON TITLE: Post Test



SAFEGUARDING PERSONAL INFORMATION

FEDERAL BUREAU OF INVESTIGATION

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)

Question 4 of 10

The requirements of the Privacy Act apply whenever agencies collect, maintain and administer records about an individual that they retrieve by the individual's name or any other unique personal identifiers. Select the best response and select SUBMIT.

- ☐ True
- ☐ False

SUBMIT

LESSON TITLE: Post Test



SAFEGUARDING PERSONAL INFORMATION

FEDERAL BUREAU OF INVESTIGATION

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)

Question 5 of 10

Which of the following scenarios violate the Privacy Act?
Select the best response and select SUBMIT.

- ☐ A. Maintaining records about a not-for-profit entity without a SORN
- ☐ B. Creating and using a Privacy Act System of Records without publishing a System of Records Notice in the Federal Register
- ☐ C. Making an individual's record available to a law enforcement agency for a criminal investigation pursuant to a published routine use
- ☐ D. Disclosing an individual's record to a third party after obtaining the individual's consent

SUBMIT

LESSON TITLE: Post-Test



SAFEGUARDING PERSONAL INFORMATION

NATIONAL SECURITY AGENCY

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)

Question 6 of 10

Which of the following is true regarding protections for PII?
Select the best response and select SUBMIT.

- ☐ A. Records that are not covered by the Privacy Act may still require protection because they contain PII.
- ☐ B. If you are located in a SCIF, it is permissible to leave PII in the open for all to see, because only cleared personnel are allowed in a SCIF.
- ☐ C. A person's name is the only PII that needs to be protected.

SUBMIT

LESSON TITLE: Post-Test

UNCLASSIFIED



SAFEGUARDING PERSONAL INFORMATION

NATIONAL CYBER INTERFERENCE CENTER

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)

Question 7 of 10

What office(s) need to know about breaches of PII that have occurred or may have occurred?
Select the best response and select SUBMIT.

- ☐ A. ODNI or NCTC Executive Secretariat
- ☐ B. ODNI Civil Liberties and Privacy Office (CLPO)
- ☐ C. Open Source Center
- ☐ D. All of the above

SUBMIT

LESSON TITLE: Post Test

UNCLASSIFIED



SAFEGUARDING PERSONAL INFORMATION

NATIONAL FEDERAL LAW ENFORCEMENT AGENCY

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)

Question 8 of 10

Which of the following is NOT a valid (authorized) disclosure of information under the Privacy Act (and thus subject to sanctions or penalties under the Privacy Act)?

Select the best response and select SUBMIT.

- ☐ A. Disclosure to Wendy Worker of her work records on file with the Federal Government, pursuant to her written Privacy Act or Freedom of Information request
- ☐ B. Disclosure of Wendy Worker's personnel records to FBI pursuant to an agency "routine use" relating to vetting of personnel
- ☐ C. Disclosure of Wendy Worker's personnel records to a contact or colleague at the FBI who believes he may have been posted with Wendy Worker during a TDY abroad a few years ago
- ☐ D. Disclosure of Wendy Worker's personnel records to the FBI based upon a signed consent form from Wendy Worker

SUBMIT

LESSON TITLE: Post Test



SAFEGUARDING PERSONAL INFORMATION

NATIONAL CENTER FOR IDENTITY PROTECTION

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)

Question 9 of 10

Which of the following collections of records would need to have a published System of Records Notice (SORN)?
Select the best response and select SUBMIT.

- ☐ A. A database of Department of Health and Human Services (HHS) Public Health doctors from which information is retrieved by area of specialty (e.g., neuroscience, nuclear science, etc.)
- ☐ B. A database of Department of Health and Human Services (HHS) Public Health doctors from which information is retrieved by the city where the doctor works (e.g., Chicago, New York, etc.)
- ☐ C. A database of Department of Health and Human Services (HHS) Public Health doctors from which information is retrieved by the name of the medical school attended (e.g., Harvard University, Johns Hopkins University, etc.)
- ☐ D. A database of Department of Health and Human Services (HHS) Public Health doctors from which information is retrieved by their individual tax ID number

SUBMIT

LESSON TITLE: Post-Test

UNCLASSIFIED



SAFEGUARDING PERSONAL INFORMATION

NATIONAL ARCHIVES AND RECORDS CENTER

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)

Question 10 of 10

Which of the following is NOT true regarding the National Security exemption under the Privacy Act?
Select the best response and select **SUBMIT**.

- ☐ A. If an agency claims the national security-related exemption under the Privacy Act for a particular System of Records, the Agency's published System of Records Notice (SORN) will reflect that fact.
- ☐ B. If any agency claims the national security-related exemption under the Privacy Act, the agency still must publish a SORN if it maintains a database of records about U.S. citizens or legal permanent residents that are retrieved by a unique personal identifier.
- ☐ C. If an agency claims the national security-related exemption under the Privacy Act for a specific System of Records the agency is no longer bound by the Privacy Act with regard to that system of records.
- ☐ D. If an agency claims the national security-related exemption under the Privacy Act, the agency may deny access to an individual who seeks to learn more about the records that the agency maintains about him.

SUBMIT

LESSON TITLE: Post Test

UNCLASSIFIED

**SAFEGUARDING PERSONAL INFORMATION**

PERSONAL AND PRIVATE INFORMATION COURSE

[MENU](#) | [GLOSSARY](#) | [RESOURCES](#)**Post Test Summary**

Congratulations! You have passed the post test!
Please review the feedback below and then hit the NEXT button to continue.

You may also find additional information by clicking on the RESOURCES and GLOSSARY buttons at the top right of the interface.

LESSON TITLE: Post Test



SAFEGUARDING PERSONAL INFORMATION
NATIONAL COURSE OF PROGRAM CENTER

GLOSSARY | RESOURCES

Certificate of Completion
NCTC Privacy Act 101
Safeguarding Personal Information

Your Name Here

15 January 2013

To print this certificate please use the "PRINT" button below.
After printing, you may exit the course by closing the browser window.

PRINT