OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

Ms. Ginger McCall
Electronic Privacy Information Center
1718 Connecticut Avenue, NW
Suite 200
Washington, D.C. 20009

Reference: DF-2012-00090; EPIC v. ODNI, Case # 1:12-cv-01282-JEB

Dear Ms. McCall:

This serves as an interim response to your 15 June 2012 letter to the Office of the Director of National Intelligence ("ODNI"), wherein you requested, under the Freedom of Information Act ("FOIA"):

1. **The guidelines and mechanisms for the correction or documentation of "inaccuracy or unreliability of [ ] information, and supplement incomplete information to the extent additional information becomes available;"**

2. **Training materials used to "ensure that [ ] personnel use the datasets only for authorized NCTC purposes and understand the baseline and enhanced safeguards, dissemination restrictions, and other privacy and civil liberties protections they must apply to each such dataset;"**

3. **Any information or documentation related to abuse, misuse, or unauthorized access of datasets acquired by NCTC (as indicated by the monitoring, recording and auditing described in Section (C)(3)(d)(3)).**

4. **Written determinations by the Director of NCTC or designee regarding "whether enhanced safeguards, procedures, and oversight mechanisms are needed."**

As subsequently negotiated with the Department of Justice, you revised your request and limited it to only records related to the revised NCTC AG Guidelines of March, 2012, and to documents that are final and not pre-decisional or deliberative in nature.

Your request was processed in accordance with the FOIA, 5 U.S.C. § 552, as amended. With respect to item 1, The ODNI was unable to locate any information responsive to your request.

With respect to item 2, four responsive documents were located and they are being released in segregable form with deletions made pursuant to FOIA Exemptions 1, 2, 3, and/or 6; 5 U.S.C. 552 §§ (b)(1), (b)(2), (b)(3), and (b)(6).

With respect to item 3, please be advised that responsive material was located by the ODNI and is currently under review, and is being coordinated with other government agencies.

We will provide a final response to this portion of your request once our reviews and external coordinations have been completed.

With respect to item 4, the ODNI was unable to locate any information responsive to your request.

Exemption 1 protects information which is currently and properly classified in accordance with Executive Order 13526. Exemption 2 protects records that relate solely to internal personnel rules and practices of an agency. Exemption 3 protects information that is specifically covered by statute. In this case, the applicable statutes are the National Security Act of 1947, as amended, 50 U.S.C. § 403-1, which protects information pertaining to intelligence sources and methods, and the Central Intelligence Agency Act of 1949, 50 U.S.C. § 403g, as amended, which protects, among other things, the names and other identifying information of personnel. Exemption 6 protects information the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

The ODNI regulation governing administrative appeals is set forth in 32 CFR § 1700.13. This regulation states that no appeal shall be accepted if the information in question is the subject of pending litigation in federal courts.

Sincerely,

John F. Hackett
Chief, Information and Data Management Group

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

Ms. Ginger McCall
Electronic Privacy Information Center
1718 Connecticut Avenue, NW
Suite 200
Washington, D.C. 20009

Reference: DF-2012-00091; EPIC v. ODNI, Case # 1:12-cv-01282-JEB

Dear Ms. McCall:

This responds to your 14 June 2012 letter to the Office of the Director of National Intelligence ("ODNI"), wherein you requested, under the Freedom of Information Act ("FOIA"), **"1. Terms and Conditions and related documents, as described in Section (B)(2)(a) of the NCTC Guidelines; and 2. All documents related to disputes between department and agency heads and DNI, as described under Section (B)(2)(d) of the NCTC Guidelines."** As subsequently negotiated with the Department of Justice, you revised your request and limited it to only records related to the revised NCTC AG Guidelines of March, 2012, and to documents that are final and not pre-decisional or deliberative in nature.

Your request was processed in accordance with the FOIA, 5 U.S.C. § 552, as amended. The ODNI was unable to locate any information responsive to your request.

The ODNI regulation governing administrative appeals are set forth in 32 CFR §1700.13. This regulation states that no appeal shall be accepted if the information in question is the subject of pending litigation in federal courts.

Sincerely,

John F. Hackett
Chief, Information and Data Management Group

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

Ms. Ginger McCall
Director, Electronic Privacy Information Center
1718 Connecticut Avenue, NW
Suite 200
Washington, D.C. 20009

Reference: DF-2012-00092; EPIC v. ODNI, Case # 1:12-cv-01282-JEB

Dear Ms. McCall:

This responds to your 15 June 2012 letter to the Office of the Director of National Intelligence ("ODNI"), wherein you requested, under the Freedom of Information Act ("FOIA"), **"[a]ny guidelines or legal memoranda discussing NCTC's understanding and interpretation of the following standards used in the NCTC Guidelines discussed above: 'reasonably believed to constitute terrorism information,' 'reasonably believed to contain terrorism information,' and 'likely to contain significant terrorism information.'"** As subsequently negotiated with the Department of Justice, you revised your request and limited it to only records related to the revised NCTC AG Guidelines of March, 2012, and to documents that are final and not pre-decisional or deliberative in nature.

Your request was processed in accordance with the FOIA, 5 U.S.C. § 552, as amended. The ODNI was unable to locate any information responsive to your request.

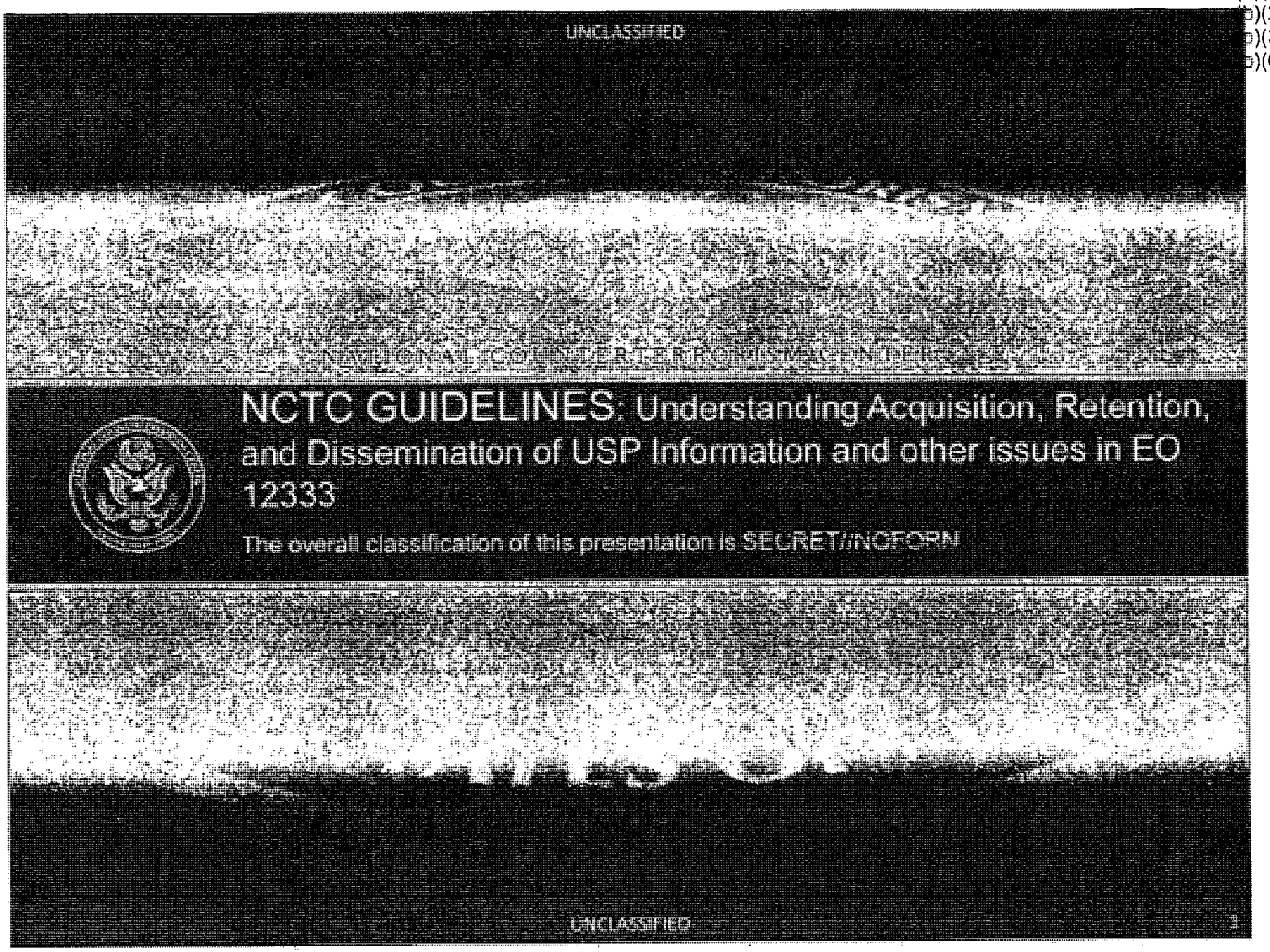
The ODNI regulation governing administrative appeals are set forth in 32 CFR §1700.13. This regulation states that no appeal shall be accepted if the information in question is the subject of pending litigation in federal courts.

Sincerely,

John F. Hackett
Chief, Information and Data Management Group

C05956033

(b)(1)
(b)(2)
(b)(3)
(b)(6)



JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Wednesday, March 24, 2010

State Department Employee Sentenced for Illegally Accessing Confidential Passport Files

A State Department employee was sentenced today to 12 months of probation for illegally accessing more than 60 confidential passport application files, Assistant Attorney General Lanny A. Breuer of the Criminal Division announced. Debra Sue Brown, 47, of Oxon Hill, Md., was also ordered by U.S. Magistrate Judge John M. Facciola in the District of Columbia to perform 50 hours of community service. Brown pleaded guilty on Dec. 11, 2009, to a one-count criminal information charging her with unauthorized computer access.

Goal

- To provide an overview of NCTC authorities
- This training:
  - Supplements the IC-wide USP training
  - Complements [redacted] and Privacy Act training (b)(1)

The procedures described here do not apply to NCTC

[redacted] (b)(1)

Module Objectives

At the end of this presentation, participants will be able to:

- Describe NCTC's mission
- Identify NCTC's authorities and its legal and policy framework
- Define NCTC collection authority under E.O. 12333
- Define "terrorism information" under IRTPA
- Describe NCTC's ability to access, acquire, retain, and disseminate information under HR 7-1 and the new AG-DNI Guidelines
- Identify the different tracks for access to information under the AG-DNI Guidelines

NCTC's Mission

- To serve as the primary organization in the USG for analyzing and integrating all intelligence possessed and acquired by the USG pertaining exclusively to terrorism and counterterrorism, excepting exclusively domestic terrorism and counterterrorism

- To serve as the central and shared knowledge bank on known or suspected terrorists

- To conduct strategic operational planning for counterterrorism activities

Sources of NCTC's Authorities

- Executive Order 12333, as amended
- National Security Act of 1947, as amended
- IRTPA, 2004

Legal and Policy Framework

- E.O. 12333 requires each IC element to have procedures implementing authorities
- CIA's HR 7-1 "Law and Policy Governing the Conduct of Intelligence Activities" (as adopted by ODNI/NCTC)
- Guidelines for Access, Retention, Use, and Dissemination by the National Counterterrorism Center and Other Agencies of Information in Datasets Containing Non-Terrorism Information (2012 Guidelines)
- NCTC Policies for access to information (Policies 3 & 4)

NCTC Authority Overview

- NCTC can receive and analyze all terrorism information possessed by the USG
- HR 7-1 provides authority for retention, use, and dissemination of USP information that is terrorism information
- NCTC may receive or access non-terrorism datasets and exclusively domestic terrorism data to determine if they contain international terrorism information (per AG-DNI Guidelines)

Acquisition - How does NCTC get the data?

- NIM/ISPPO leads the acquisition process
- Acquisition, retention, and dissemination are controlled by two documents:
  - HR 7-1
  - 2012 Attorney General – DNI Guidelines

Acquisition - Which Guidelines Control?

- Datasets composed of terrorism information will presumptively be covered by HR 7-1
- Dataset "inherently USP in nature" will presumptively be covered by the 2012 Guidelines
- Determination made based on:
  - where it was gathered from
  - direct knowledge of the records in the database, or
  - by reasonable implication based on the type of activity that resulted in the collection of the data

- Determination made by ISPPO in consultation with NCTC Legal and the Civil Liberties and Privacy Officer (CLPO)

2012 AG-DNI Guidelines Overview

- The 2012 AG-DNI Guidelines permit:
  - NCTC to ***access*** or ***acquire*** US Person information for the purpose of determining whether the information is ***reasonably believed*** to constitute terrorism information
  - To ***retain*** US Person information when it is ***reasonably believed*** to constitute terrorism information

Terrorism Information

- Broad meaning of "terrorism information" (IRTPA)
  - Existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism
  - Threats posed by such groups or individuals
  - Groups or individuals reasonably believed to be assisting or associated with such groups
  - Includes WMD information

How does NCTC get the data under the AG-DNI Guidelines?

Track 1: Role-based Access

- Access to datasets containing non-terrorism information
- Access essentially the same as that of employees of the data holder
- Once information is identified as terrorism information, NCTC may retain and use for authorized purposes
- US Person information that is not terrorism information will be purged from NCTC systems

How does NCTC get the data under the AG-DNI Guidelines?

Track 2: Queries Performed by Other Agencies

Data provider retains custody and control of the data

- Performs searches at the request of NCTC
- Queries must be based on terrorism data-points
- Queries should be reasonably expected to return terrorism information results
- Terrorism information discovered through this process may be retained and used for authorized purposes

How does NCTC get the data under the AG-DNI Guidelines?

Track 3: Data set replication/Ingestion

- NCTC may acquire and replicate portions or the entirety of datasets when necessary to identify the information that constitutes terrorism information
  - Reasonable efforts to mark USP information
  - USP information may be retained and assessed for up to five years
  - Subject to agreements with data providers, other restrictions
  - Subject to baseline safeguards, possibly enhanced safeguards
  - USP information that is terrorism information may be used for NCTC purposes, as outlined under the Guidelines

Track 3 - Dataset Replication/Ingestion (cont'd)

- These datasets are maintained in restricted-access repositories and:
  - Are subject to monitoring, recording, and auditing requirements
    - Tracking of logons/logoffs
    - Tracking of queries executed

Track 3 - Baseline Safeguards

- Queries are conducted solely to identify information that is reasonably believed to constitute terrorism information
- Queries shall be designed to minimize the review of information about US Persons that does not constitute terrorism information
- ***Once terrorism information is identified***:
  - Retain, use and disseminate in accordance with NCTC authorities
  - Adhere to any data handling requirements attached to the dataset in which the terrorism information was identified

Track 3 - Enhanced Safeguards

- The Director of NCTC -- in consultation with ODNI/OGC and ODNI/CLPO -- decides whether enhanced safeguards are warranted for a given dataset
- Types of enhanced safeguards include:
  - Additional procedures to restrict searches, access or dissemination
  - Use of privacy-enhancing technologies

Dissemination of USP Information Under Track 1,2, and 3

- Reasonably appears to be TI or necessary to understand or assess TI

- NCTC may disseminate US person information to the IC and foreign or international entities
  - In support of FBI and DHS to other federal (Title 50), state, local, tribal entities

Dissemination (cont'd)

- Dissemination of non-TI for a limited purpose (to assess if TI)
  - Must consult with ISPPO and Legal

- Dissemination of a bulk dataset or significant portion

Compliance, Oversight, and Reporting

- *2012 AG-DNI Guidelines include enhanced controls, audit procedures, and monitoring*
  - NCTC must conduct periodic reviews of compliance, including spot checks, reviews of audit logs, etc.
  - NCTC must report "significant failures" to comply with applicable requirements
  - NCTC must prepare a comprehensive annual compliance report

Compliance, Oversight, and Reporting (cont'd)

- USP information erroneously obtained by NCTC will be promptly removed from NCTC systems unless otherwise prohibited by law

- NCTC cannot access, retain or disseminate USP information solely for the purpose of monitoring the exercise rights protected by the Constitution or other laws

Data Covered by HR 7-1

- USP Information that is acquired by means other than through the methods described in the AG-DNI Guidelines are governed by HR 7-1 *Guidance for CIA Activities within the United States*

- *For retention and dissemination purposes HR 7-1 distinguishes between information about USPs and USP Identity information*

- *Two Requirements to Disseminate Identity information outside the IC:*
  - Is it foreign intelligence?
  - Is the identity information necessary to understand or assess the intelligence?

DO	DON'T
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

If you're not sure, ask Legal

Questions?

How to Find NCTC Legal

[redacted] (b)(2) (b)(3)

[redacted] (b)(2) (b)(3)

[redacted] (b)(2) (b)(3) (b)(6)

Additional Resources

Civil Liberties and Privacy Office:

[redacted] (b)(2) (b)(3) (b)(6)

Information Sharing Program and Policy:

[redacted] (b)(2) (b)(3) (b)(6)

Backup Slides

Refresher: Definition of US Person

	Text of EO 12333	IS	IS NOT
1	A United States citizen…	One born in the US or naturalized as a citizen; includes dual citizen	Foreign citizen; Visa holder
2	…an alien known by the intelligence element concerned to be a permanent resident alien…	Green card holder; where "known" with due diligence	Student visa holder; most immigrants (asylee or refugee)
3	…an unincorporated association substantially composed of United States citizens or permanent resident aliens…	Not-for-profit group or social club with USP majority	Not-for-profit group or social club where USPs are not majority
4	…a corporation incorporated in the United States, except a corporation directed and controlled by a foreign government or governments.	US legal corporation. US legally established subsidiary of a foreign (non-gov't) corporation.	Foreign corporation or foreign gov't directed/controlled.

12333 and NCTC Collection

REMEMBER:

"OVERTLY OR THROUGH PUBLICLY AVAILABLE SOURCES"

- Remember Undisclosed Participation rules...
- Apply similar rules for on-line registration as conference registration
- Overt means you must disclose ODNI affiliation when interacting with US Persons on-line to obtain information
- Publicly available means information that is published or broadcast for public consumption, accessible on-line or otherwise to the public, or is available to the public by subscription or purchase

Undisclosed Participation

Per EO 12333:

- No one acting on behalf of an element of the IC may join or otherwise participate in any organization in the US on behalf of any element of the IC without disclosing their intelligence affiliation to appropriate officials of the organization
- Prohibited from influencing the activity of the organization or its members

- Applies to participation in the US
- Must disclose if required as a condition of attendance.

12333 and NCTC Use of the Internet

REMEMBER:

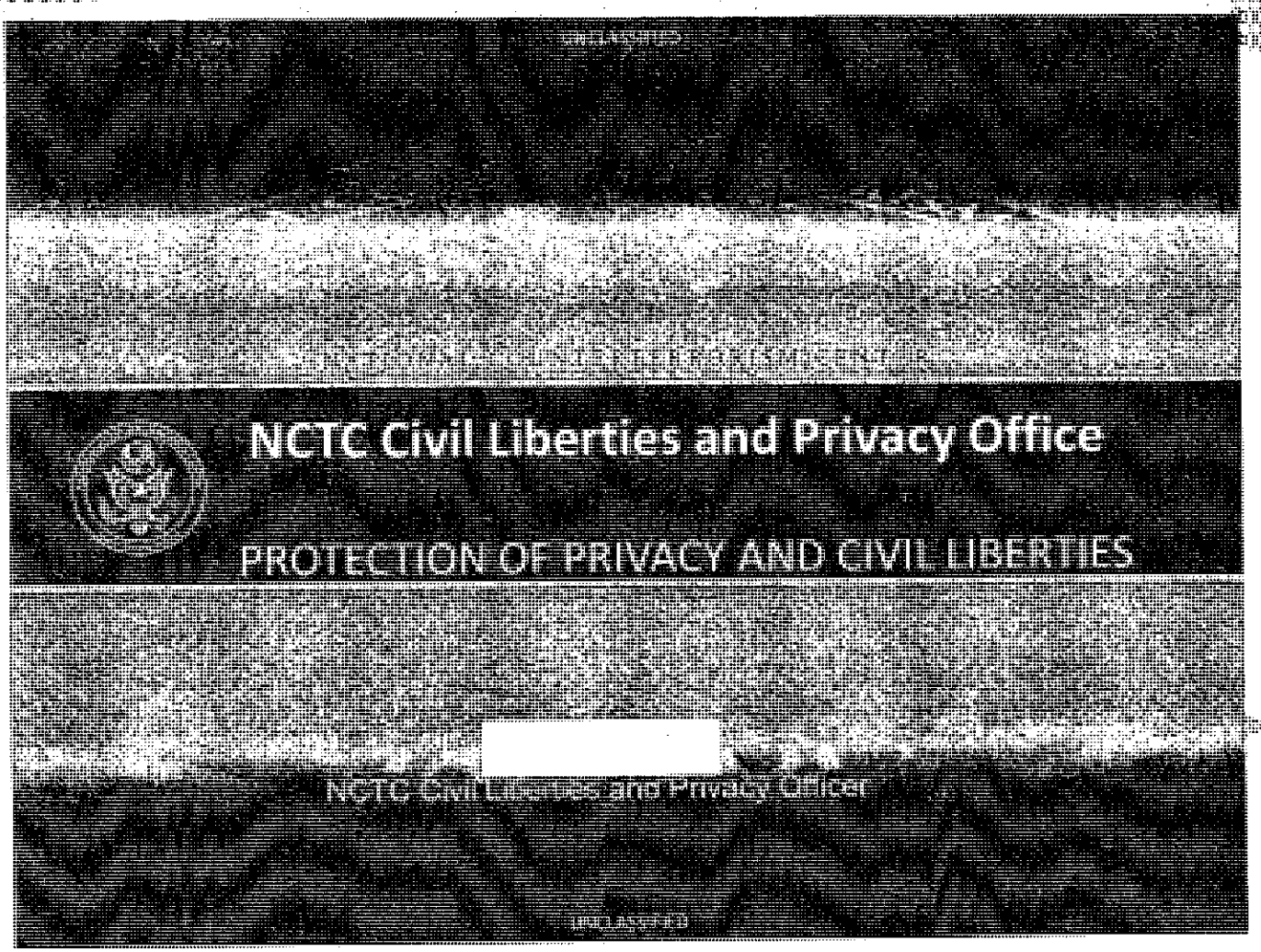
"OVERTLY OR THROUGH PUBLICLY AVAILABLE SOURCES"

- Web Searches/Data Aggregation/Social Sites
  - Must be services that are generally available to the public
    - Still requires terrorism predicate
    - Must be cognizant of CI and operational concerns
    - What browser are you using?
- Cannot use classified information for search terms
- May not use alias/pen names
- May not obscure IC affiliation to register and view information not otherwise available to the general public

12333 and NCTC Use of the Internet

- May not browse for information based on the exercise of constitutionally protected rights
- Remember that HR 7-1 rules for retention and dissemination of USP information apply to collected publicly available information

C05955997


NCTC Civil Liberties and Privacy Office
PROTECTION OF PRIVACY AND CIVIL LIBERTIES
[redacted]
NCTC Civil Liberties and Privacy Officer

NATIONAL COUNTERTERRORISM CENTER

Why a CLPO?

- Outside of the Intelligence Community ("IC"), there are many additional oversight mechanisms that provide for transparency:
  - Legal process/burdens of proof –and - court review (less likely to have "state secrets" defense at their disposal)
  - access by the public (and media) to records, including through redress mechanisms
  - independent watchdog organizations, public advocacy groups, etc.
  - Congress (i.e., not limited to the traditional Intel Committees)

SECRECY

There are limitations on what the government can disclose. (essential for the protection of intelligence sources and methods)

TRANSPARENCY

The **"civil liberties protection infrastructure" provides a proxy for transparency**. It is this interrelationship between legal requirements, guidelines, compliance standards, and oversight that ensures the Intelligence Community operates in a manner that protects privacy and civil liberties.

"We all share in the responsibility to ensure that our efforts to combat terrorism adhere to the laws and policies that protect the privacy and civil liberties of Americans. I appreciate your commitment to fulfill that responsibility."

NCTC Director Mott Olsen (January 10, 2012)

US Person Protections

- The key mechanisms for the protection of civil liberties and privacy within the IC emanate from 2 primary sources: Executive Order ("EO") 12333 and the Privacy Act. You'll be receiving detailed training on both in the near future.

- For now, just be aware that:

  - EO 12333 and the Privacy Act are designed to preserve the privacy of US Persons ("USPs), and to ensure that we protect and preserve each USP's constitutionally protected rights

  - In order to implement EO 12333, each IC entity adopts Attorney General Guidelines (AGGs)
    - At NCTC we have 2 sets of AGGs ; CIA's AGGs (applied to terrorism datasets) and NCTC's own AGG's (applied to datasets provided by non-IC USG agencies)

  - Some of our mission partners require us to extend USP Protection to non-USPs
    - these requirements should be highlighted for you within the context of your work with such a dataset

Civil liberty and privacy considerations in data access

- As part of our counter-terrorism ("CT") mission we acquire and analyze data for many sources. Some of this data comes from non-IC agencies, like the Depts. of Homeland Security & State
  - people engaging in every day activities, like traveling on a plane or applying for a passport
  - We often refer to these as "non-terrorism datasets"

- There are a number of privacy and civil liberties considerations implicated when we ingest this data (sometimes referred to as concerns about "Big Data")
  - potential for "mission creep," data obsolescence, and misuse/abuse/theft of data
  - Americans also have a general level of discomfort with the IC holding their data

- Ability to demonstrate that we diligently follow our privacy and civil liberties protections is critical to earning and retaining the trust of the American people/oversight entities/mission partners

- So long as we maintain this trust, we continue to have access to this critical data
  - If we lose that trust we risk losing access to the data

First Amendment Issues

- A core CL/P protection is that our focus on an individual cannot be based solely on the exercise of a constitutional right, such as a person's first amendment right to free speech

- It's therefore helpful to ask 2 questions when looking at speech:

  1) Why are we focused on this individual? For example, we're interested in this person because.....
     a) s/he is donating to a charity associated with terrorism;
     b) s/he is communicating with someone as part of an ongoing plot to conduct an attack
     c) s/he is a known associate of a known or suspected terrorist ("KST")

  2) Why is the speech relevant to this focus?
     a) e.g., speech demonstrates this person's knowledge that the charity funnels $ for terrorism
     b) e.g., speech shows that the person is directing the individual to commit an act of imminent violence
     c) e.g., speech demonstrates familiarity with, or access to, the KST

- So long as the underlying focus of our analytic judgment/action is based on more than just the protected speech itself, than it is permissible to use that speech

Compliance

- **Compliance (and compliance incidents reviews) are normal parts of the oversight process and necessary to preserve/earn the public's trust**

- Compliance incidents may be:
  - one-off occurrences (e.g., a typo in a database query caused by simple human error); or
  - ongoing occurrences (e.g., unauthorized personnel having access to an NCTC information technology system)

- We have regular compliance obligations – such as spot checks, audits and reporting

- Compliance is designed to: "trust and verify" and to correct mistakes and fix broken processes

- If we have zero (0) compliance incidents it means either:
  - we're not checking, or
  - our compliance oversight processes are broken

CLPO Take-Away

- Terrorists target the US because of our ideals, our freedoms and our constitutional way of life

- Your mission is to prevent terrorists from assailing these very ideals through the conduct of physical attacks

- CLPOs mission is to ensure that in preventing these attacks, we don't unintentionally infringe on the very constitutional rights that we are trying to protect
  - Thus, our job is to help you spot potential issues, and tackle challenges you encounter, so that together we can ensure the safety of our homeland and our way of life

- At the end of the day, we all have the very same vision/mission

Contact Information

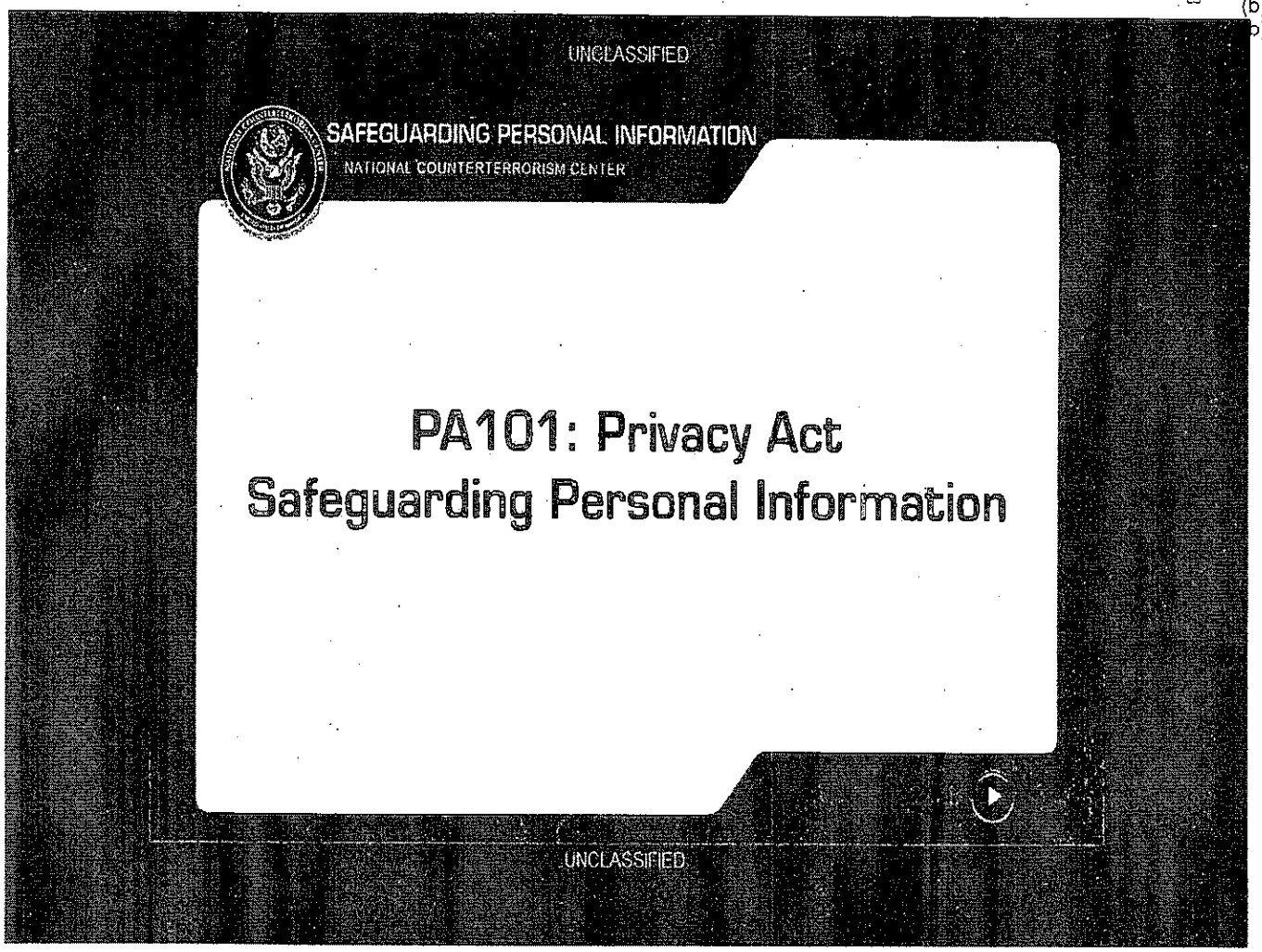
[redacted] NCTC Civil Liberties and Privacy Officer

[redacted]

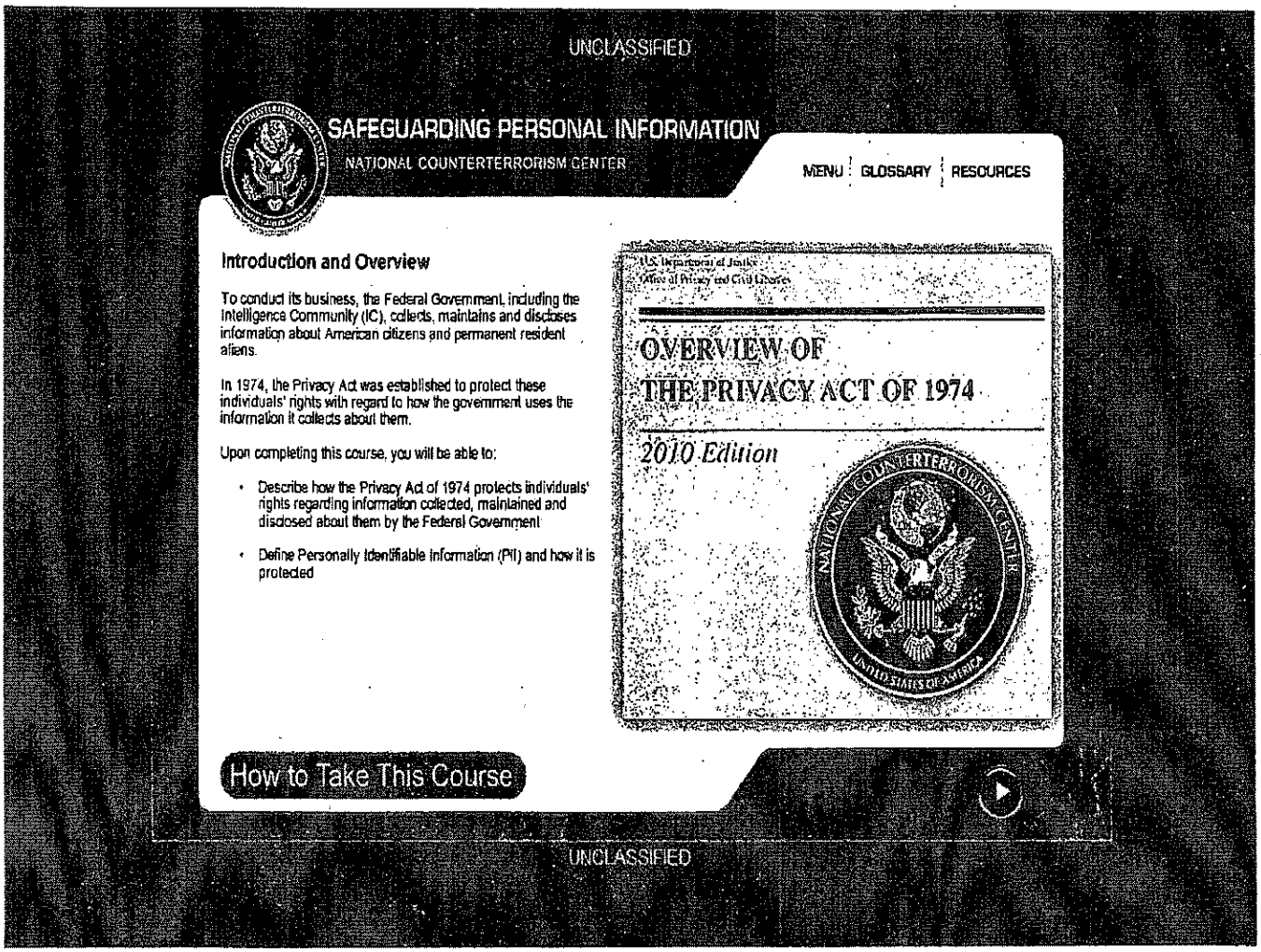
(b)(2)
(b)(3)
(b)(6)

C05956031

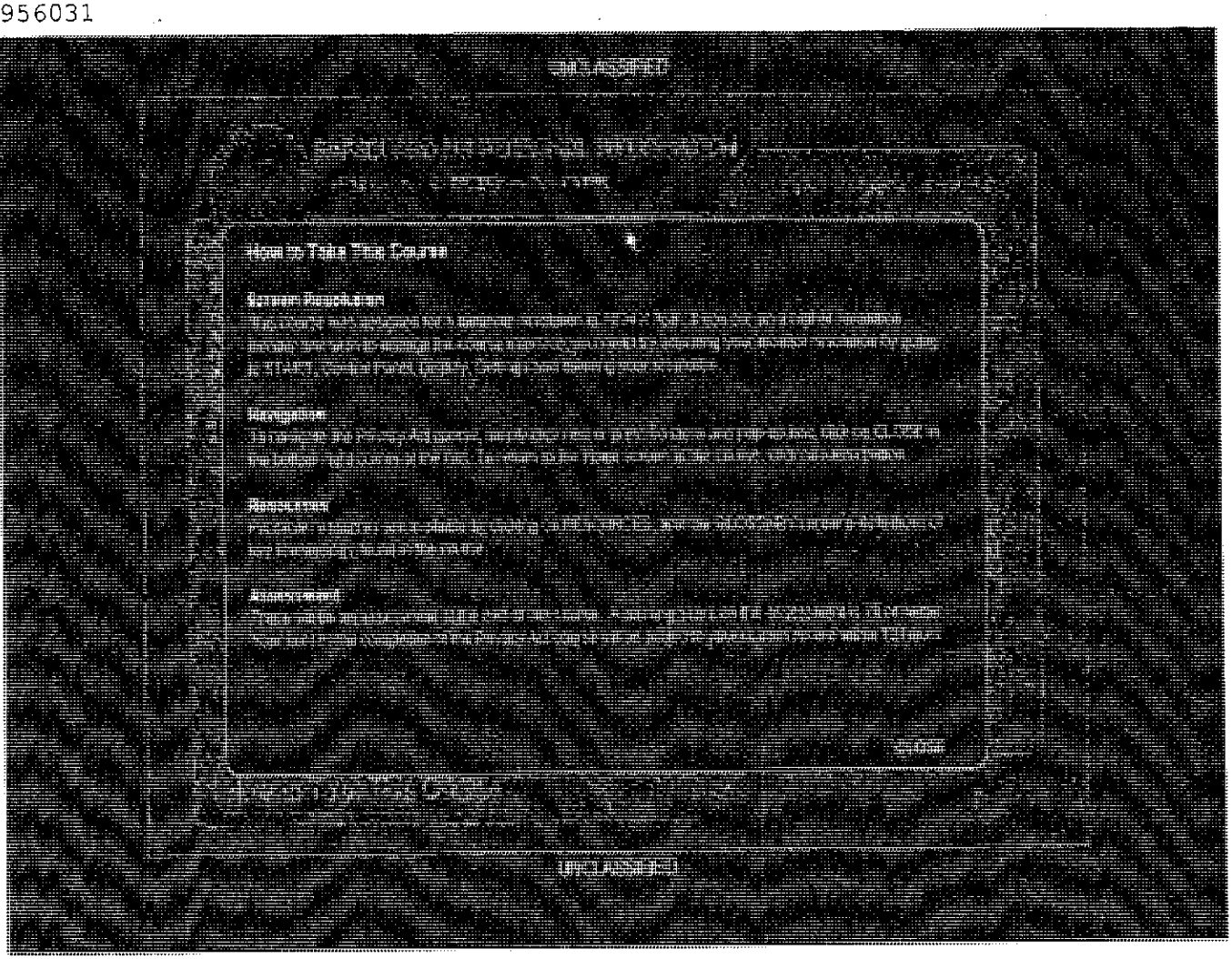
(b)(2)
(b)(3)



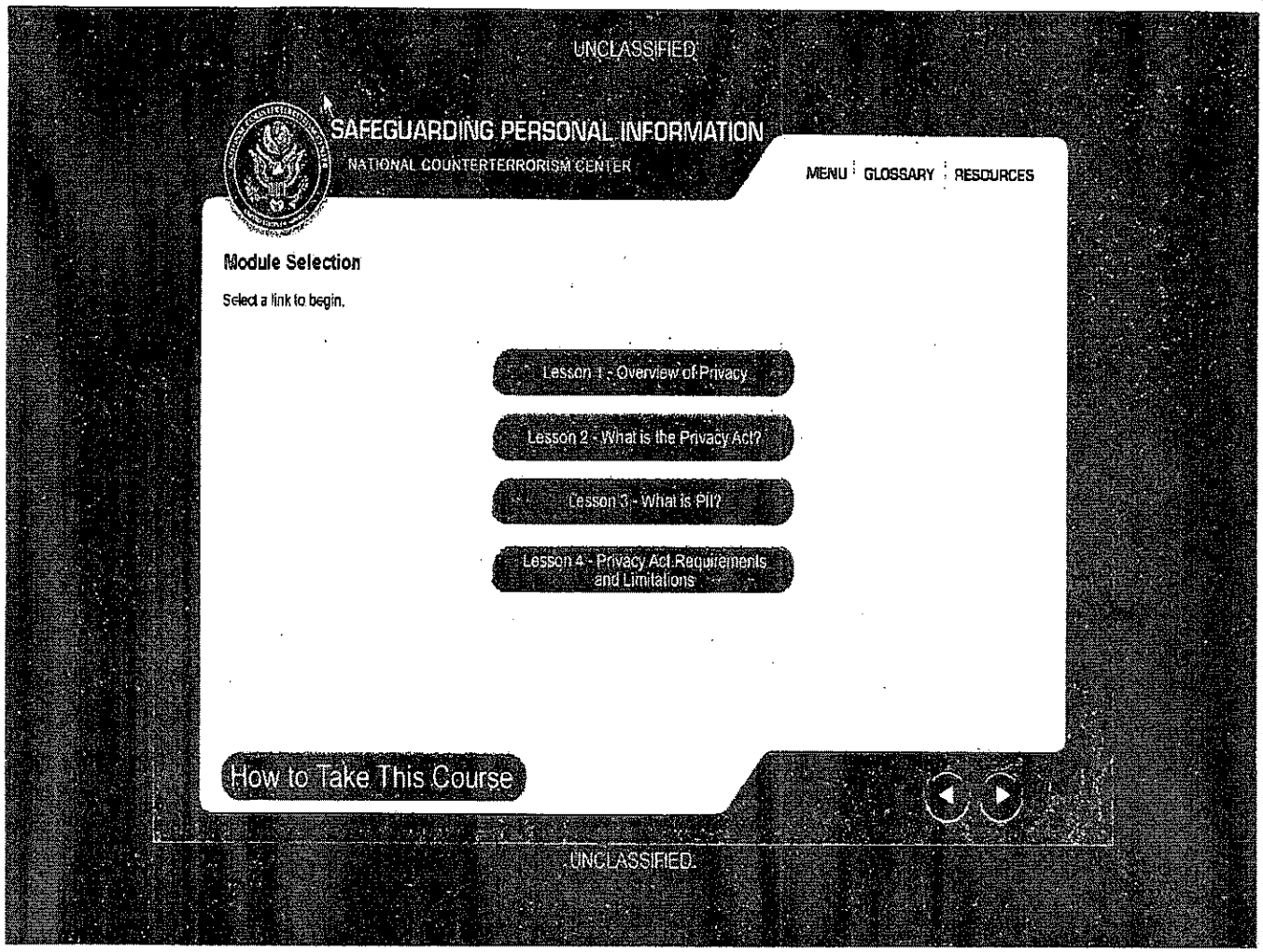
C05956031


UNCLASSIFIED
SAFEGUARDING PERSONAL INFORMATION
NATIONAL COUNTERTERRORISM CENTER
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
OVERVIEW OF
THE PRIVACY ACT OF 1974
2010 Edition
How to Take This Course
UNCLASSIFIED

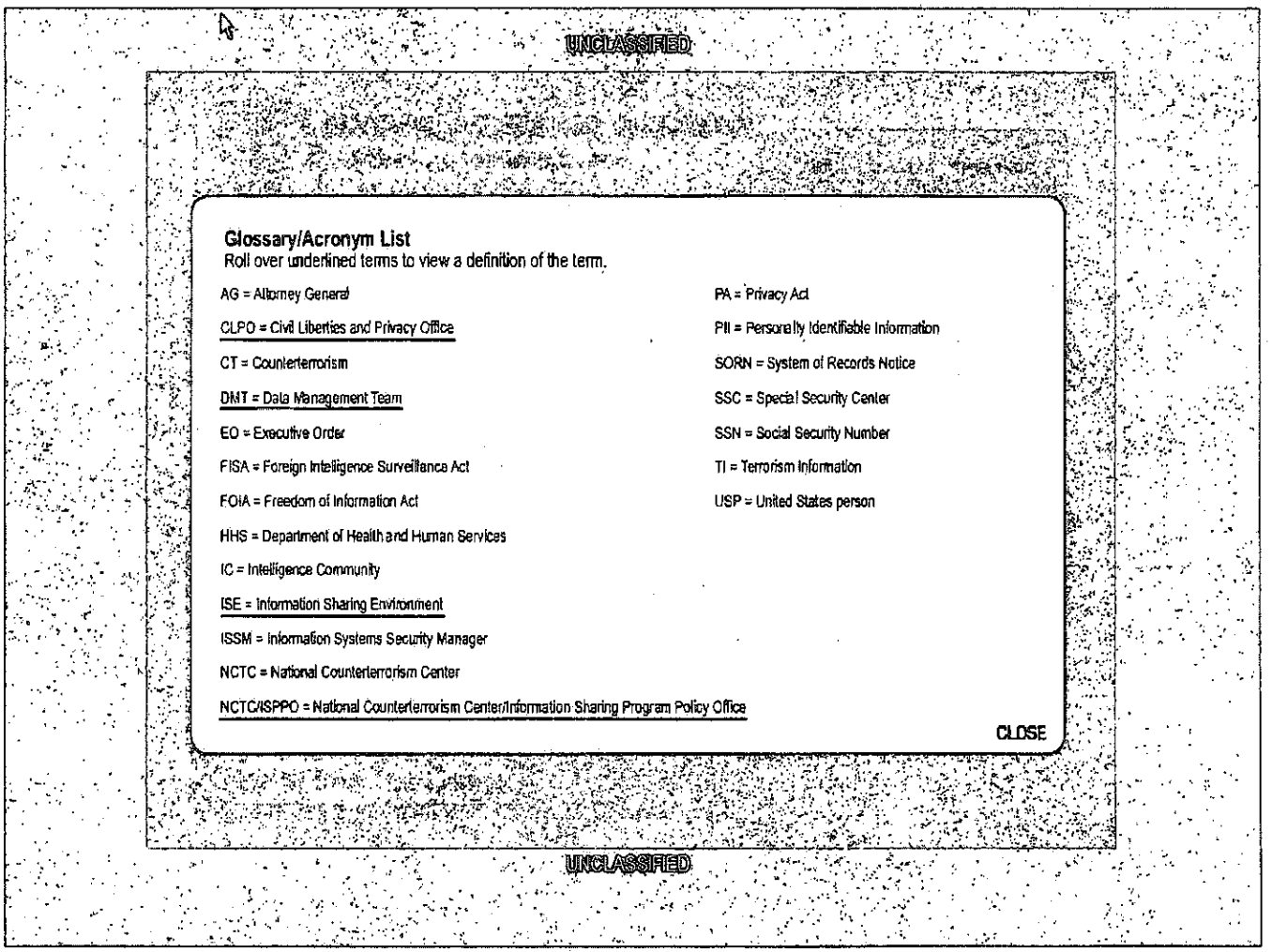
C05956031



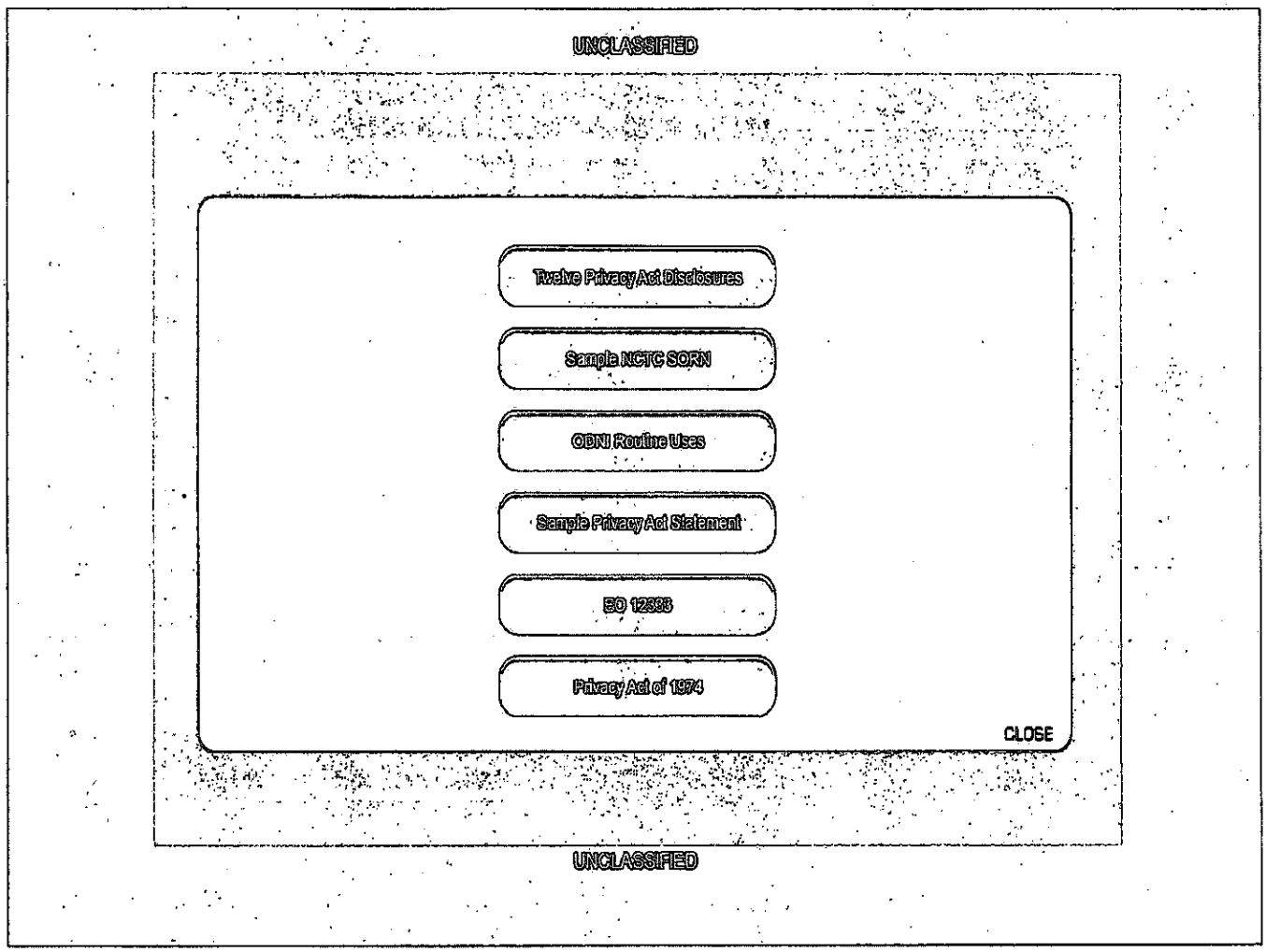
C05956031


UNCLASSIFIED
SAFEGUARDING PERSONAL INFORMATION
NATIONAL COUNTERTERRORISM CENTER
MENU | GLOSSARY | RESOURCES
Module Selection
Select a link to begin.
Lesson 1 - Overview of Privacy
Lesson 2 - What is the Privacy Act?
Lesson 3 - What is PII?
Lesson 4 - Privacy Act Requirements and Limitations
How to Take This Course
UNCLASSIFIED

C05956031


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/ISPPO = 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

C05956031


UNCLASSIFIED
Twelve Privacy Act Disclosures
Sample NCTC SORN
ODNI Routine Uses
Sample Privacy Act Statement
EO 12333
Privacy Act of 1974
CLOSE
UNCLASSIFIED

C05956031

UNCLASSIFIED

SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERTERRORISM CENTER

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.

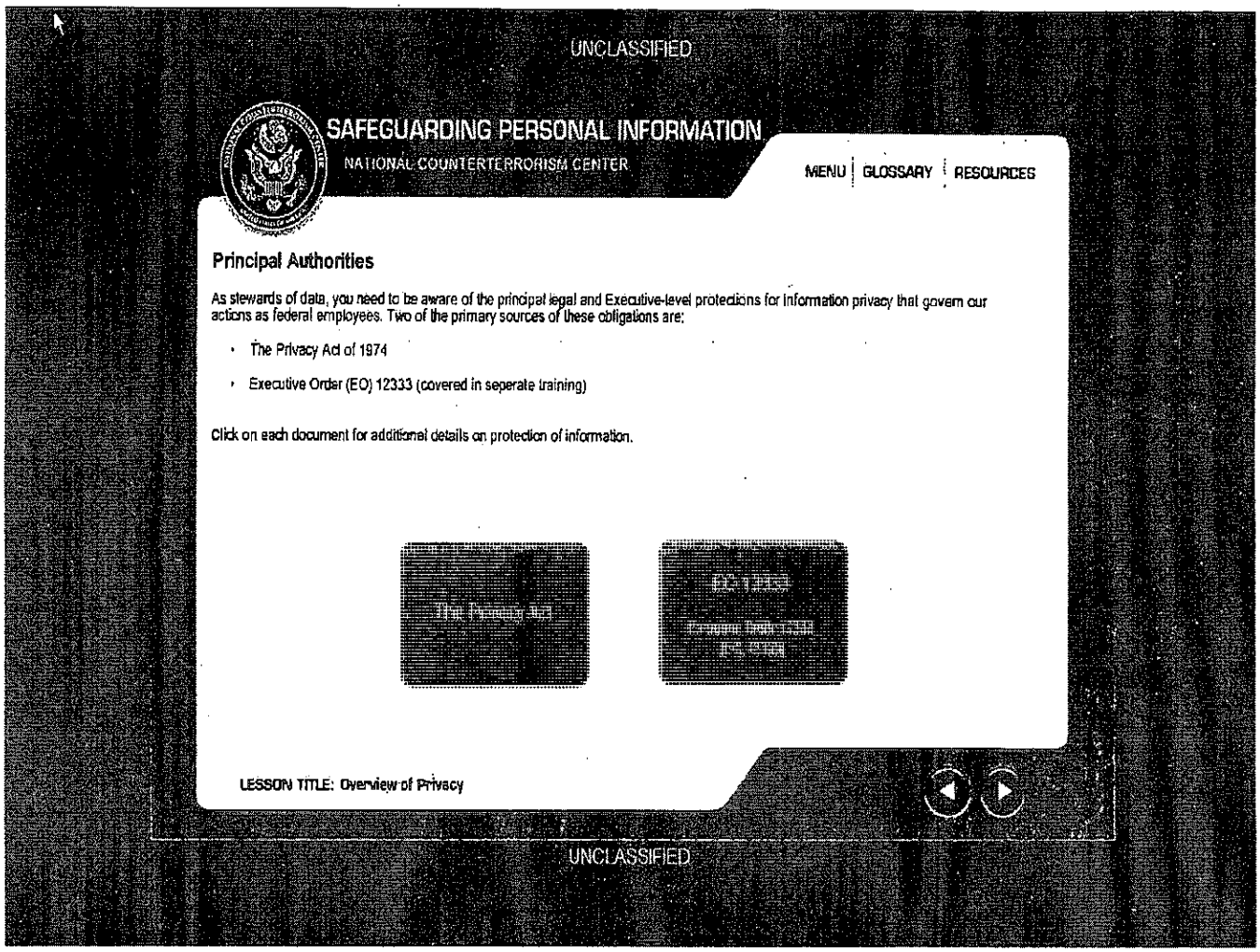
Upon completing this lesson, you will be able to:

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

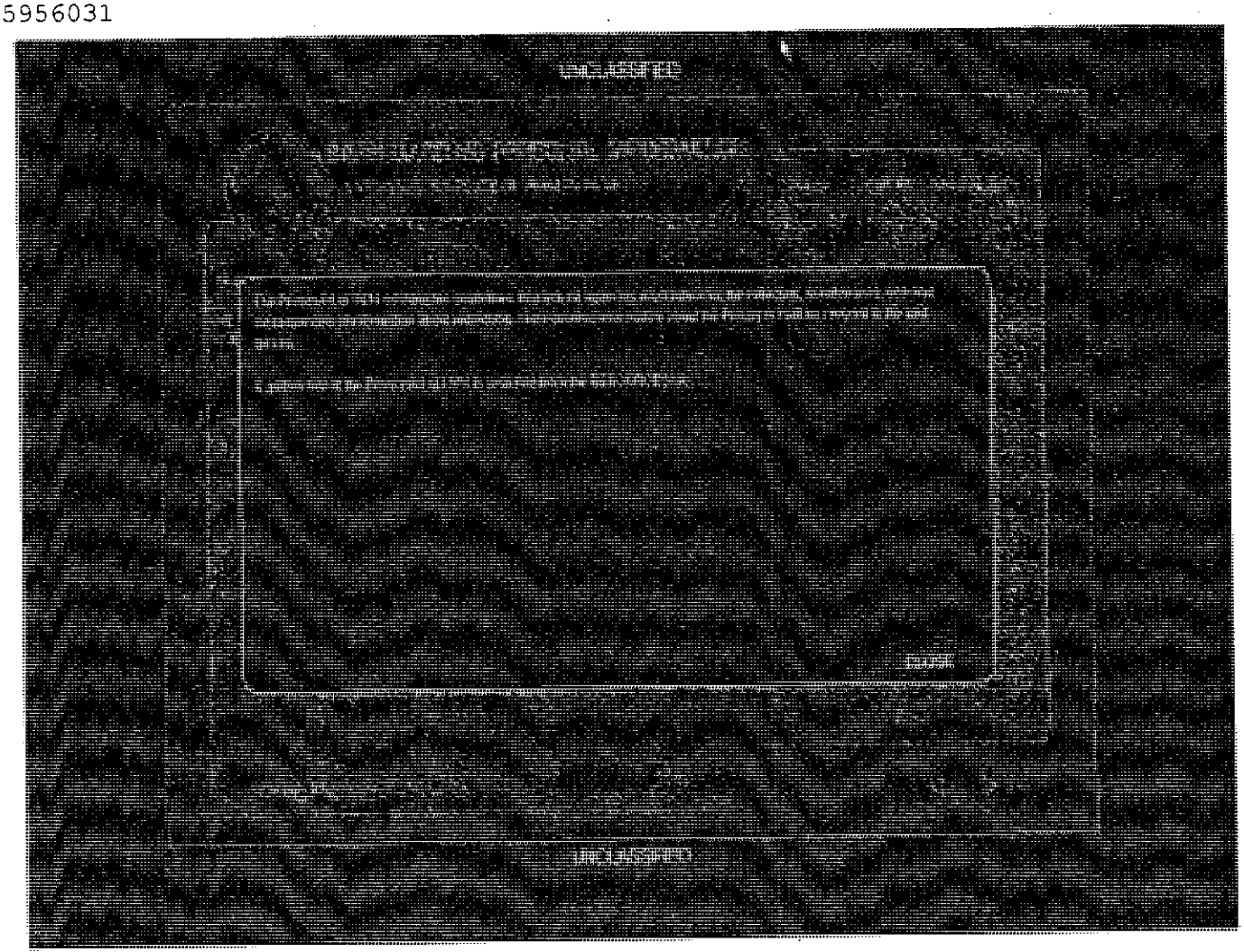
LESSON TITLE: Overview of Privacy

UNCLASSIFIED

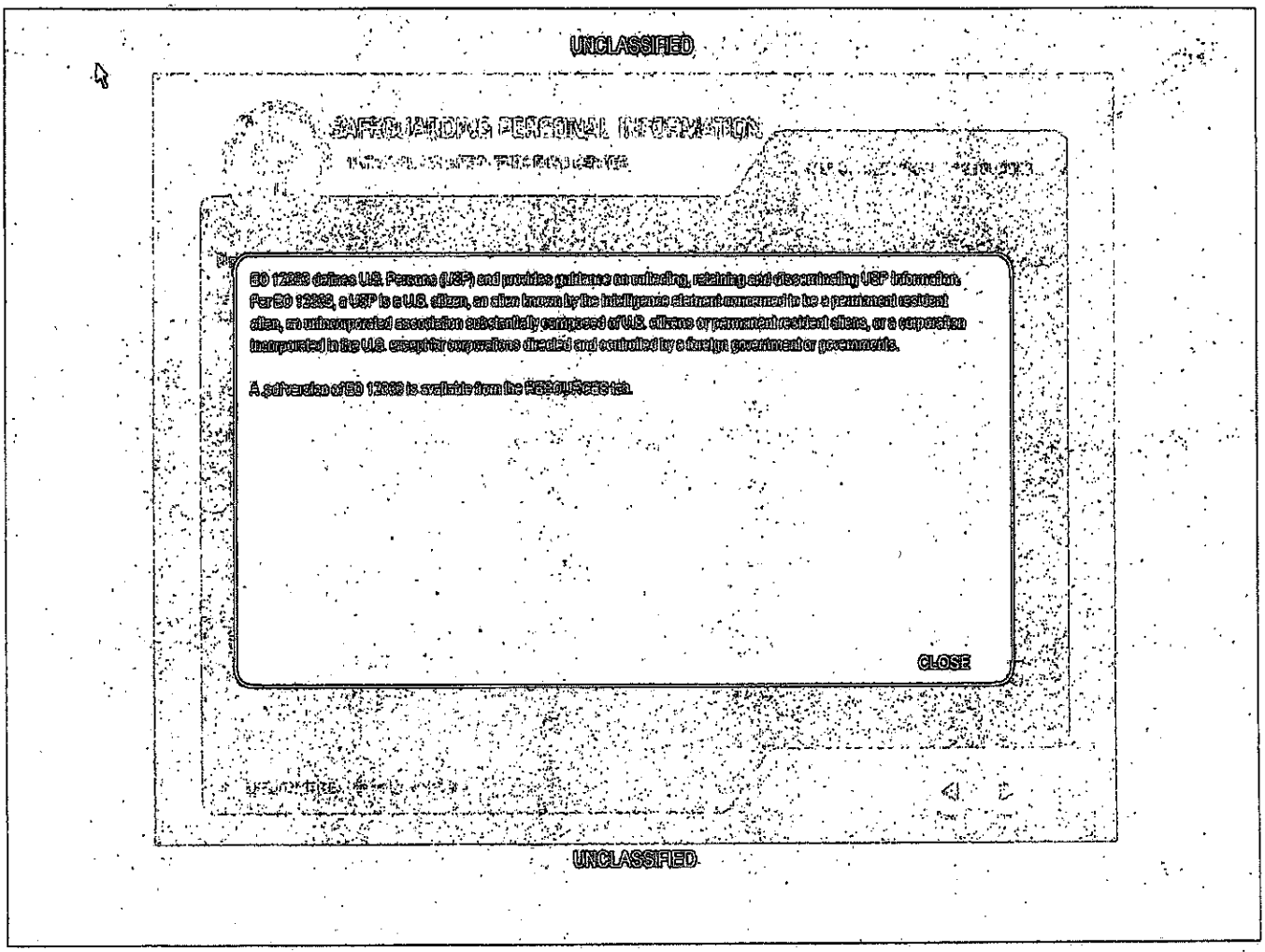
C05956031


UNCLASSIFIED
SAFEGUARDING PERSONAL INFORMATION
NATIONAL COUNTERTERRORISM 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 seperate training)
Click on each document for additional details on protection of information.
LESSON TITLE: Overview of Privacy
UNCLASSIFIED

C05956031



C05956031


UNCLASSIFIED
EO 12333 defines U.S. Persons (USP) and provides guidance on collecting, retaining and disseminating USP information.
Per EO 12333, a USP is a U.S. citizen, an alien known by the intelligence element concerned to be a permanent resident
alien, an unincorporated association substantially composed of U.S. citizens or permanent resident aliens, or a corporation
incorporated in the U.S. except for corporations directed and controlled by a foreign government or governments.
A softversion of EO 12333 is available from the [illegible]
CLOSE
UNCLASSIFIED

C05956031

UNCLASSIFIED

SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERTERRORISM CENTER

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

UNCLASSIFIED

C05956031

UNCLASSIFIED

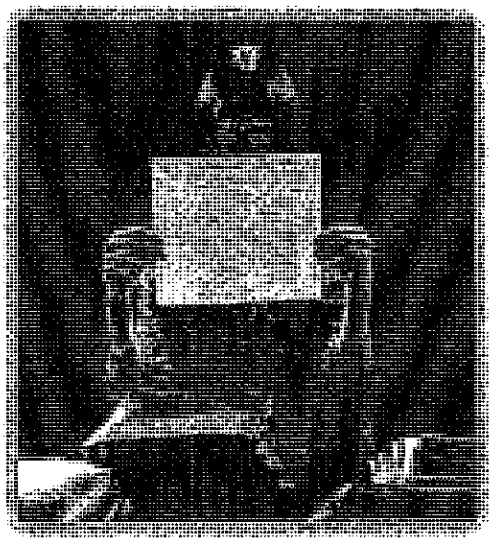
SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERTERRORISM CENTER

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

UNCLASSIFIED

C05956031

UNCLASSIFIED

SAFEGUARDING PERSONAL INFORMATION

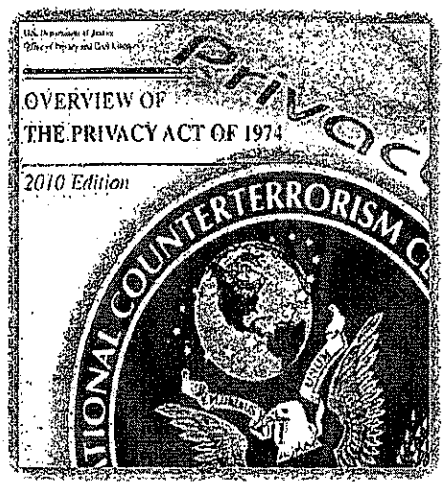
NATIONAL COUNTERTERRORISM CENTER

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?

UNCLASSIFIED

C05956031

UNCLASSIFIED

SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERTERRORISM CENTER

The Privacy Act

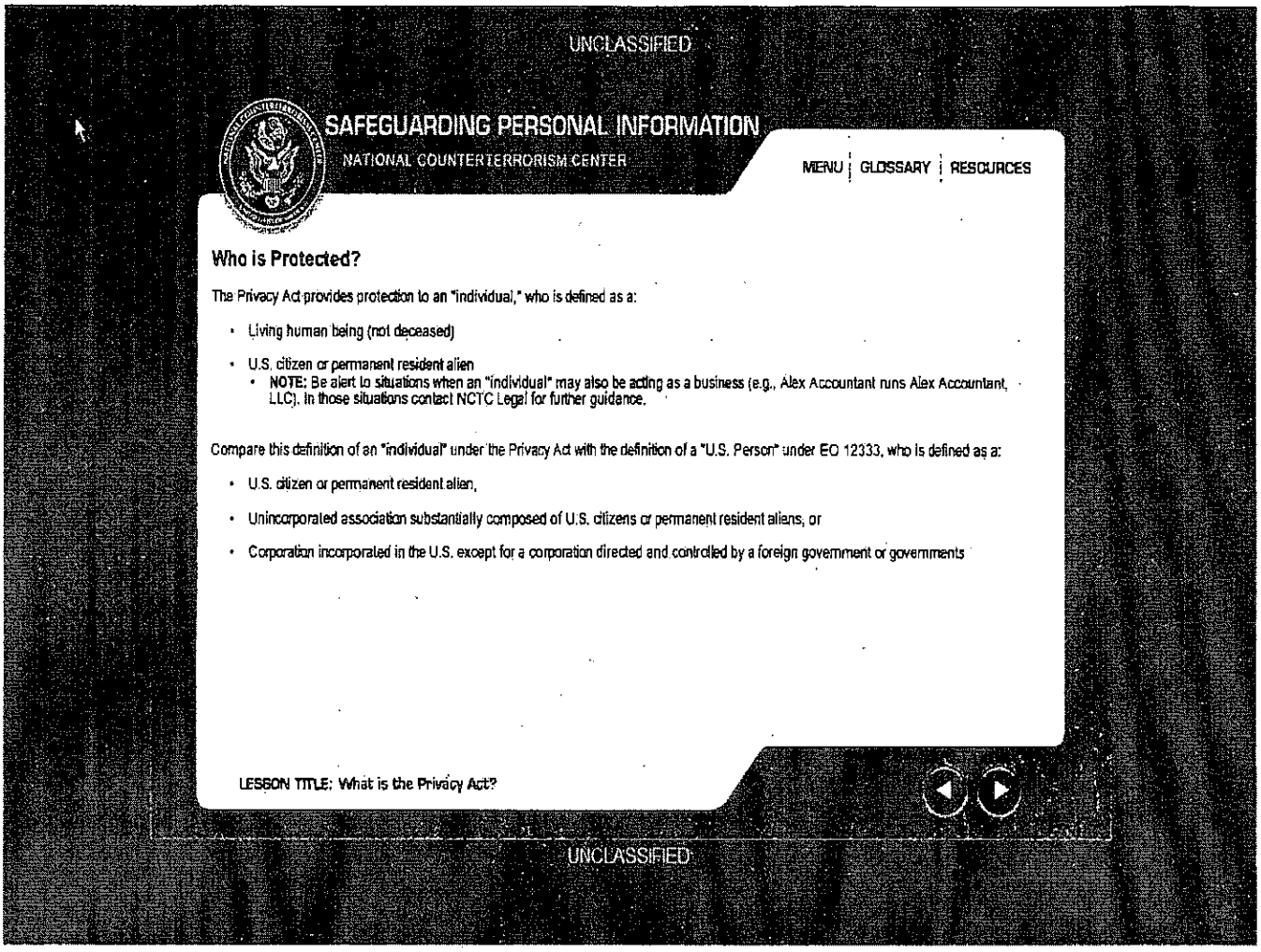
Prior to enactment of the Privacy Act in 1974, there were instances when some law enforcement and intelligence agencies inappropriately collected and used information about U.S. citizens.

The purpose of the Privacy Act is to:

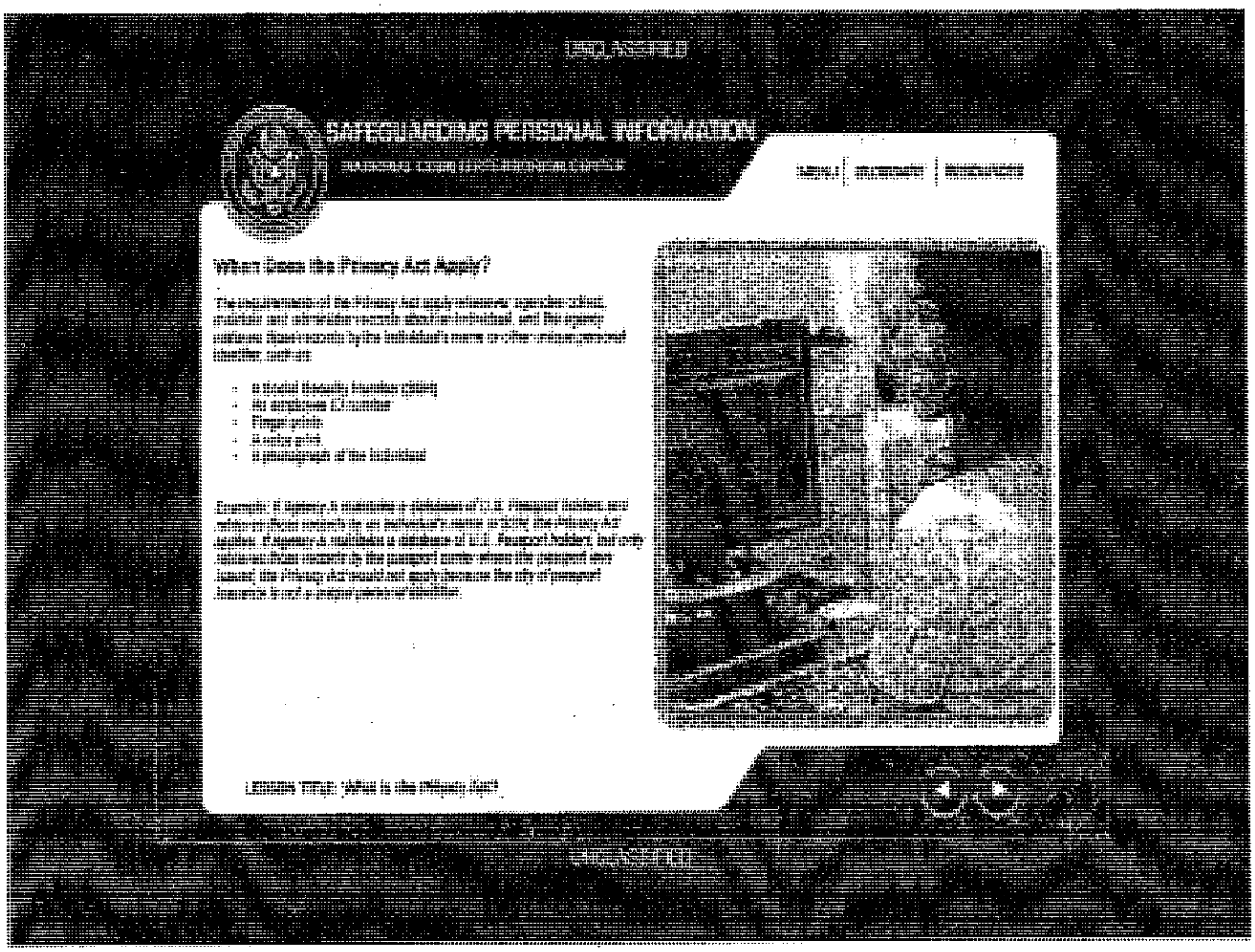
- Protect against illegal secret collection of records by the government
- Govern collection, maintenance and disclosure of information about individuals
  - The Privacy Act does not apply to statistical or aggregate information where the individual cannot be identified, such as census data or data collected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

UNCLASSIFIED

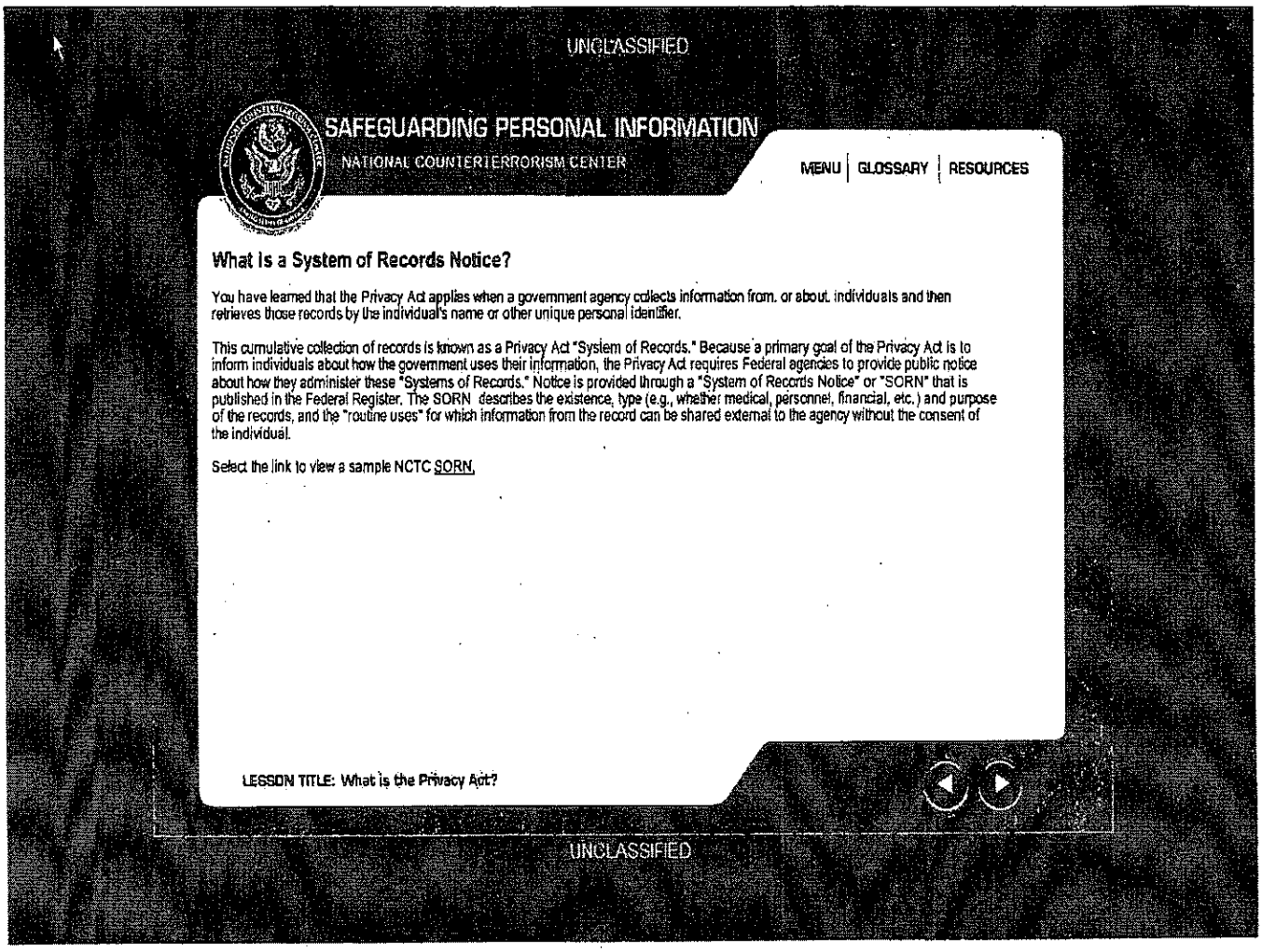
C05956031


UNCLASSIFIED
SAFEGUARDING PERSONAL INFORMATION
NATIONAL COUNTERTERRORISM 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?
UNCLASSIFIED

C05956031


SAFEGUARDING PERSONAL INFORMATION
What Does the Privacy Act Apply?

C05956031


UNCLASSIFIED
SAFEGUARDING PERSONAL INFORMATION
NATIONAL COUNTERTERRORISM CENTER
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?
UNCLASSIFIED

C05956031

UNCLASSIFIED

SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERTERRORISM CENTER

MENU | GLOSSARY | RESOURCES

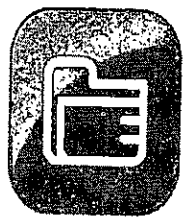
Collection of Records

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

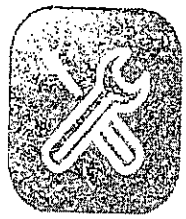
- Collect the information directly from the individual, when feasible.
- Provide individuals with a "Privacy Act Statement" at the time of collection (i.e., notice of the legal authority under which the government is collecting the information and how the government intends to use that information).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

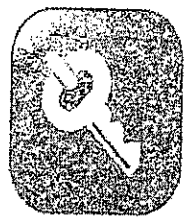
Select the link to view a sample Privacy Act Statement



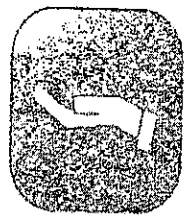
COLLECTION



MAINTENANCE



ACCESS



DISCLOSURE

LESSON TITLE: What is the Privacy Act?

UNCLASSIFIED

C05956031

UNCLASSIFIED

SAFEGUARDING PERSONAL INFORMATION

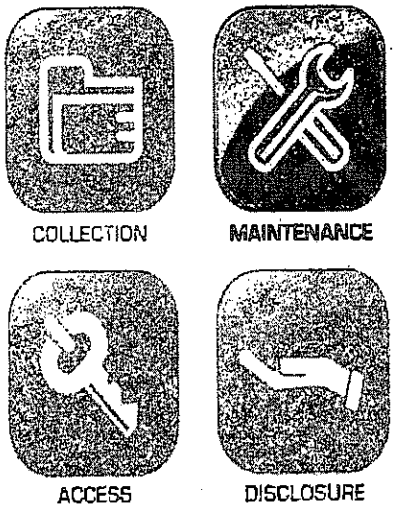
NATIONAL COUNTERTERRORISM CENTER

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.



UNCLASSIFIED

C05956031

UNCLASSIFIED

SAFEGUARDING PERSONAL INFORMATION

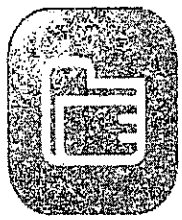
NATIONAL COUNTERTERRORISM CENTER

MENU | GLOSSARY | RESOURCES

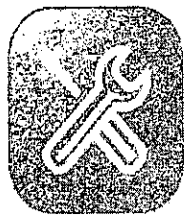
Individuals' Access to Records

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.

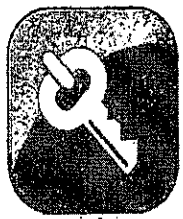
For additional information about how or whether individuals can gain access to records about themselves, consult NCTC Legal or the NCTC Civil Liberties and Privacy Office (CLPO).



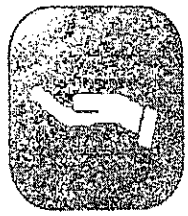
COLLECTION



MAINTENANCE



ACCESS



DISCLOSURE

LESSON TITLE: What is the Privacy Act?

UNCLASSIFIED

C05956031

UNCLASSIFIED

SAFEGUARDING PERSONAL INFORMATION

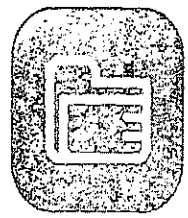
NATIONAL COUNTERTERRORISM CENTER

Disclosure or Dissemination of Records

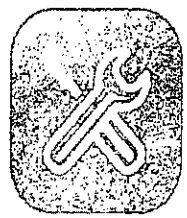
Agencies may only disclose or disseminate Privacy Act records (maintained in a System of Records) outside the agency in the following circumstances:

- With the consent of the record subject.
- For the twelve excepted 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.

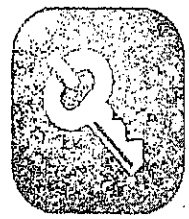
Select the link for a sample of routine uses from the ODNI Privacy Act Regulation.



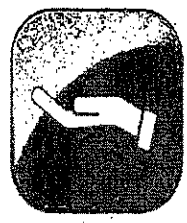
COLLECTION



MAINTENANCE



ACCESS

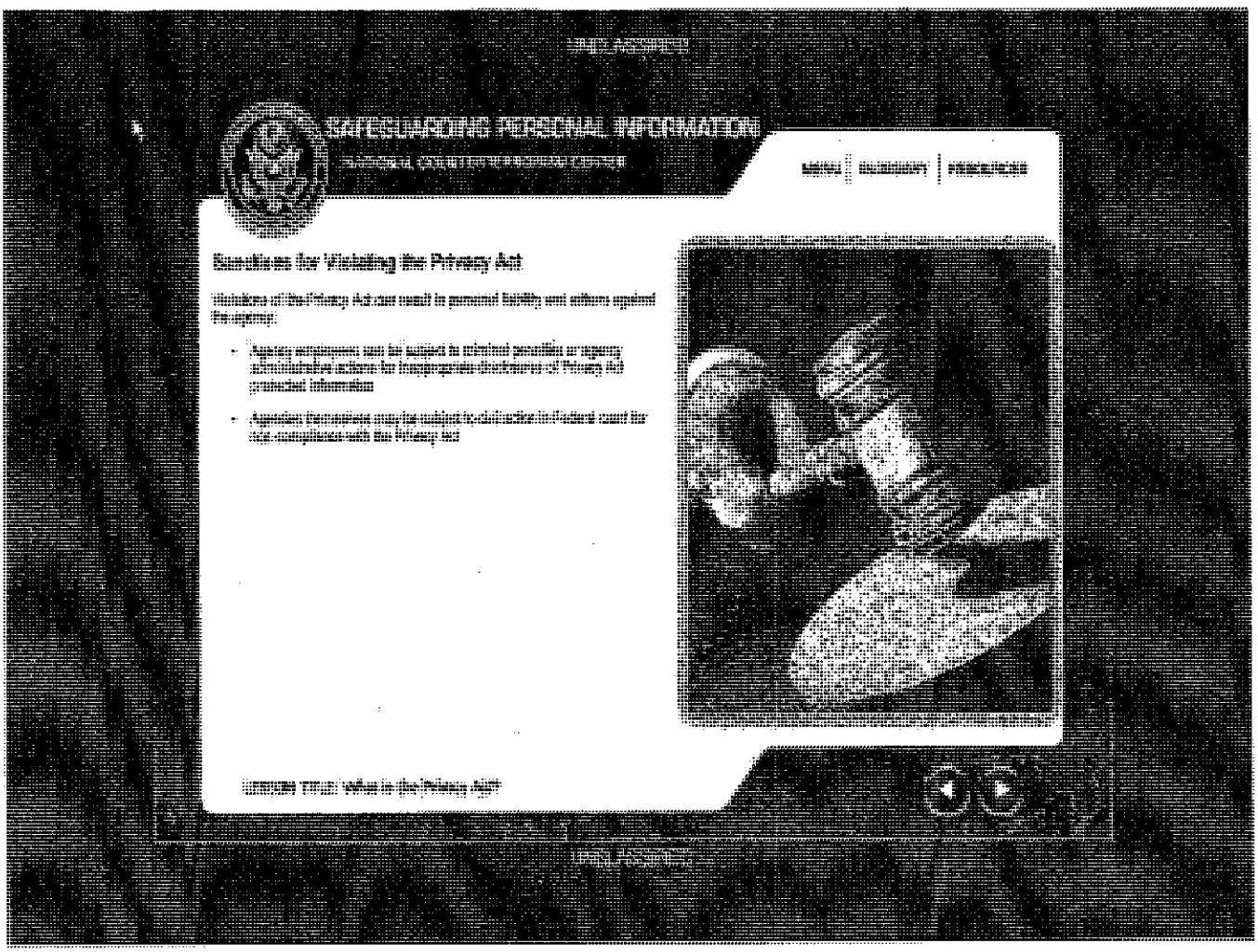


DISCLOSURE

LESSON TITLE: What is the Privacy Act?

UNCLASSIFIED

C05956031



C05956031

SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERTERRORISM CENTER

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.

C05956031

UNCLASSIFIED

SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERTERRORISM CENTER

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?

UNCLASSIFIED

C05956031

UNCLASSIFIED

SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERTERRORISM CENTER

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?

UNCLASSIFIED

C05956031

UNCLASSIFIED

SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERTERRORISM CENTER

What is Personally Identifiable Information (PII)?

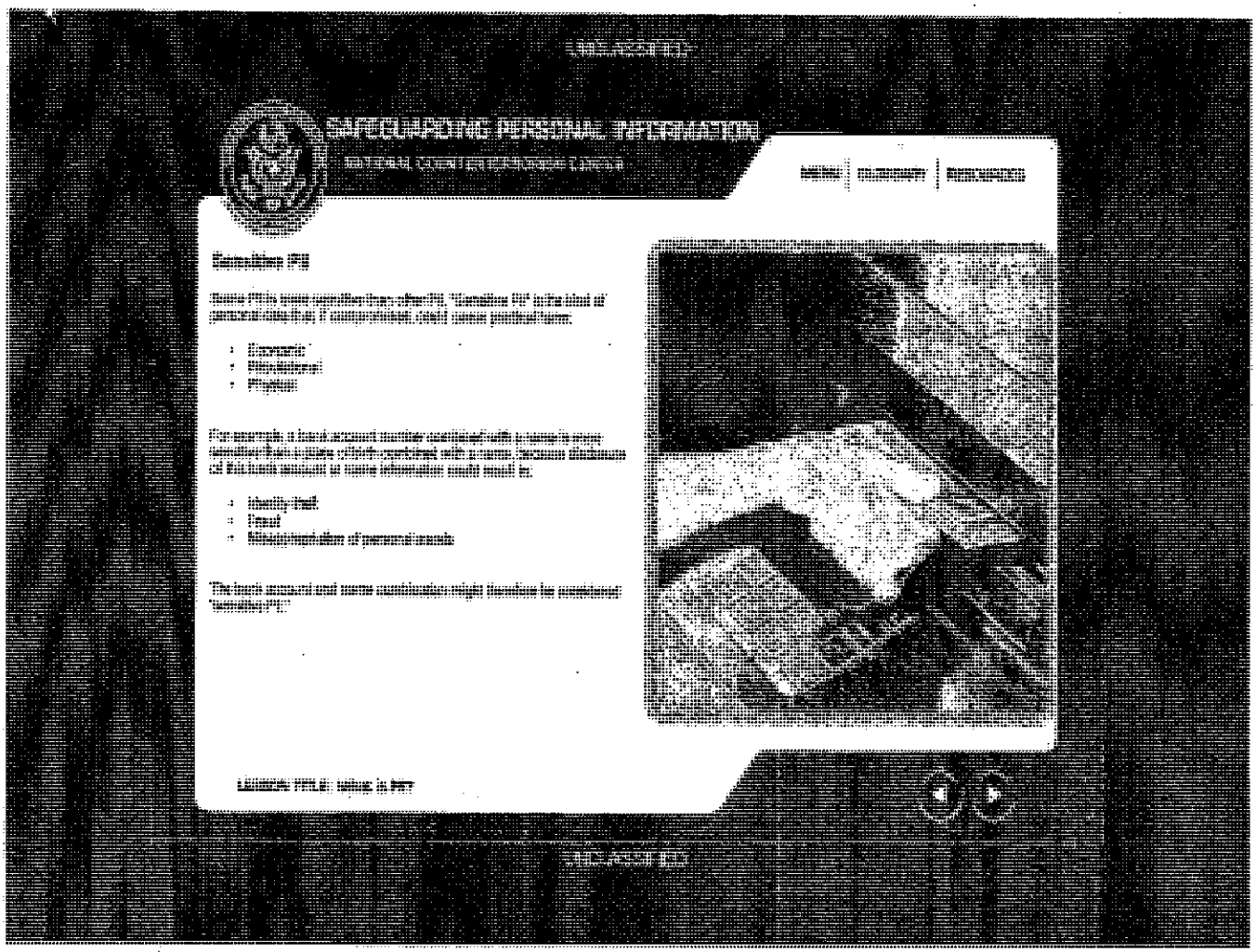
The term PII is defined in OMB Memorandum M-07-16 as:

> *"...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.

C05956031



C05956031

UNCLASSIFIED

SAFEGUARDING PERSONAL INFORMATION

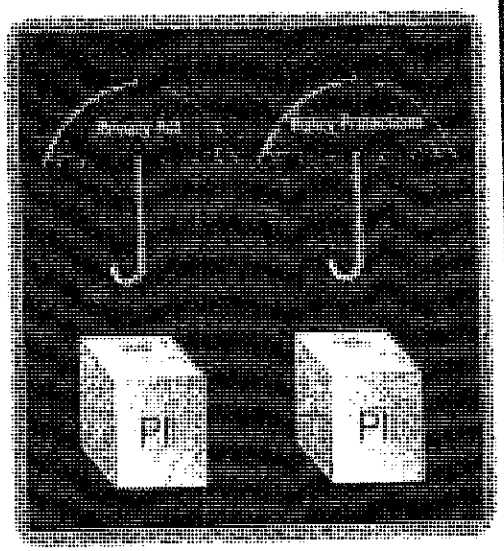
NATIONAL COUNTERTERRORISM CENTER

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.



UNCLASSIFIED

C05956031

SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERTERRORISM CENTER

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.

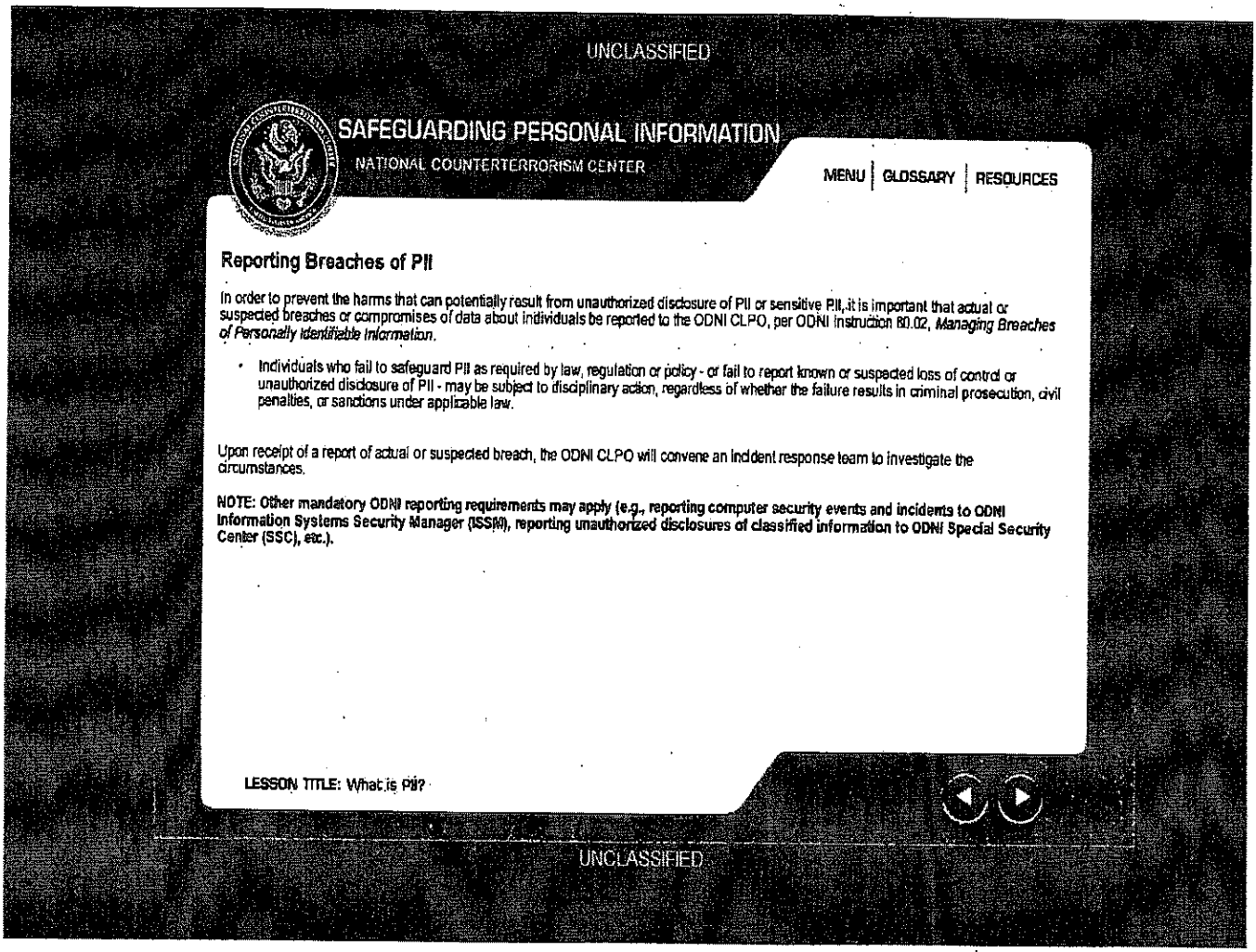
These safeguards limit records access to only those who have an authorized purpose. They also protect against threats or hazards to the security or integrity of the PII, which could result in harm, embarrassment, inconvenience or unfairness to any individual about whom the information pertains.

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.

C05956031


UNCLASSIFIED
SAFEGUARDING PERSONAL INFORMATION
NATIONAL COUNTERTERRORISM CENTER
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?
UNCLASSIFIED

C05956031

UNCLASSIFIED

SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERTERRORISM CENTER

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 IRTPA (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.

UNCLASSIFIED

C05956031

SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERTERRORISM CENTER

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)

SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERTERRORISM CENTER

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 [redacted]

b)(2)
b)(3)

C05956031

UNCLASSIFIED

SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERTERRORISM CENTER

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?

UNCLASSIFIED

C05956031

UNCLASSIFIED

SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERTERRORISM CENTER

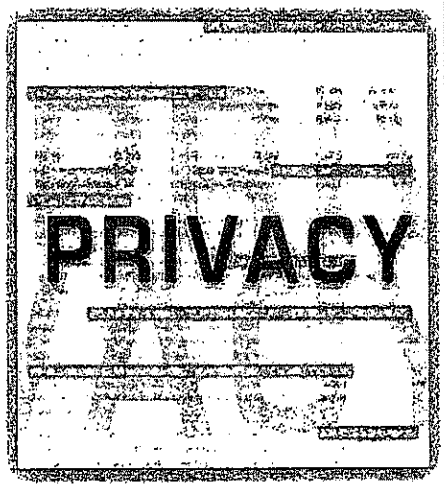
Introduction and Overview

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:

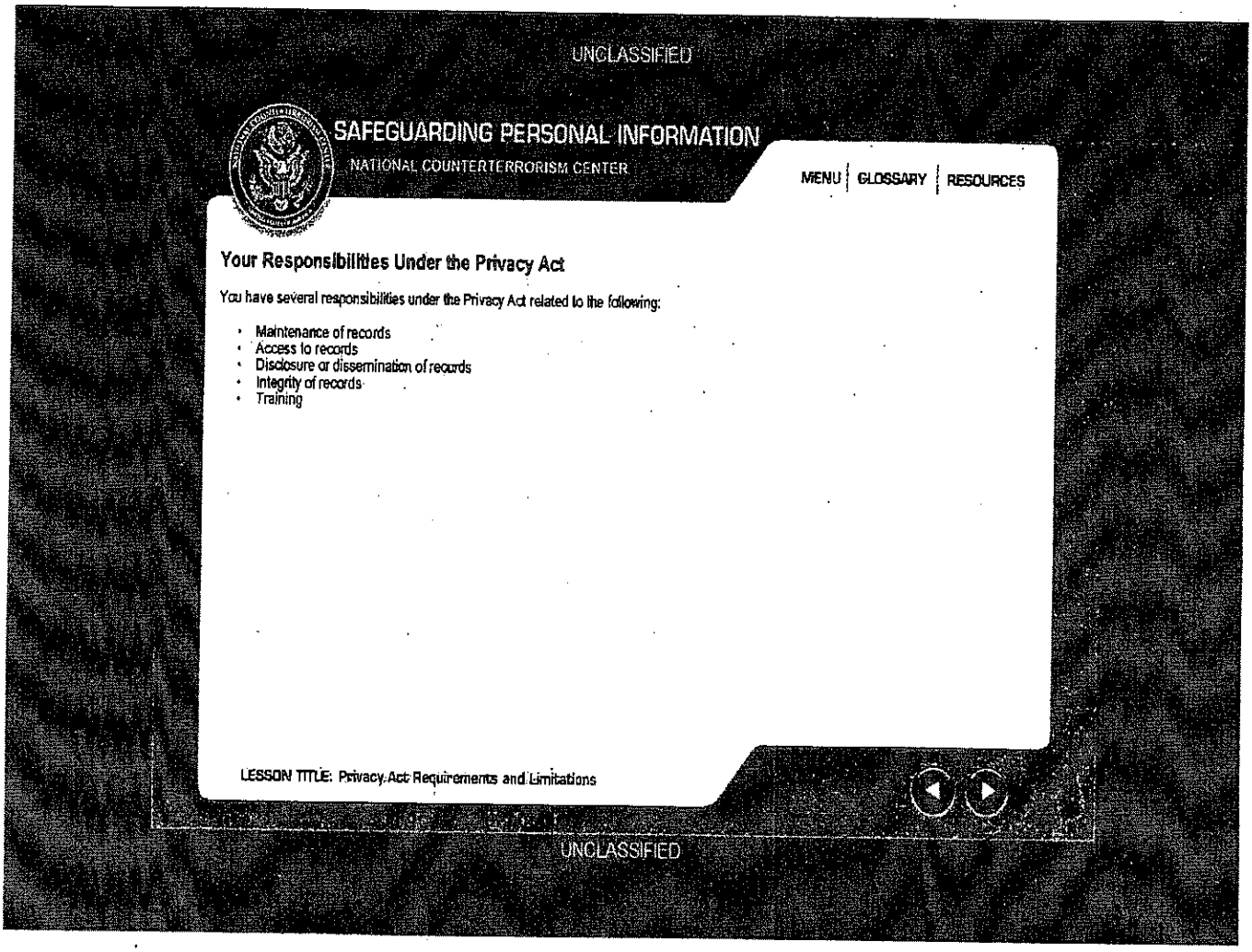
- Identify those requirements or prohibitions of the Privacy Act that may apply to you personally as you perform your day-to-day duties and responsibilities



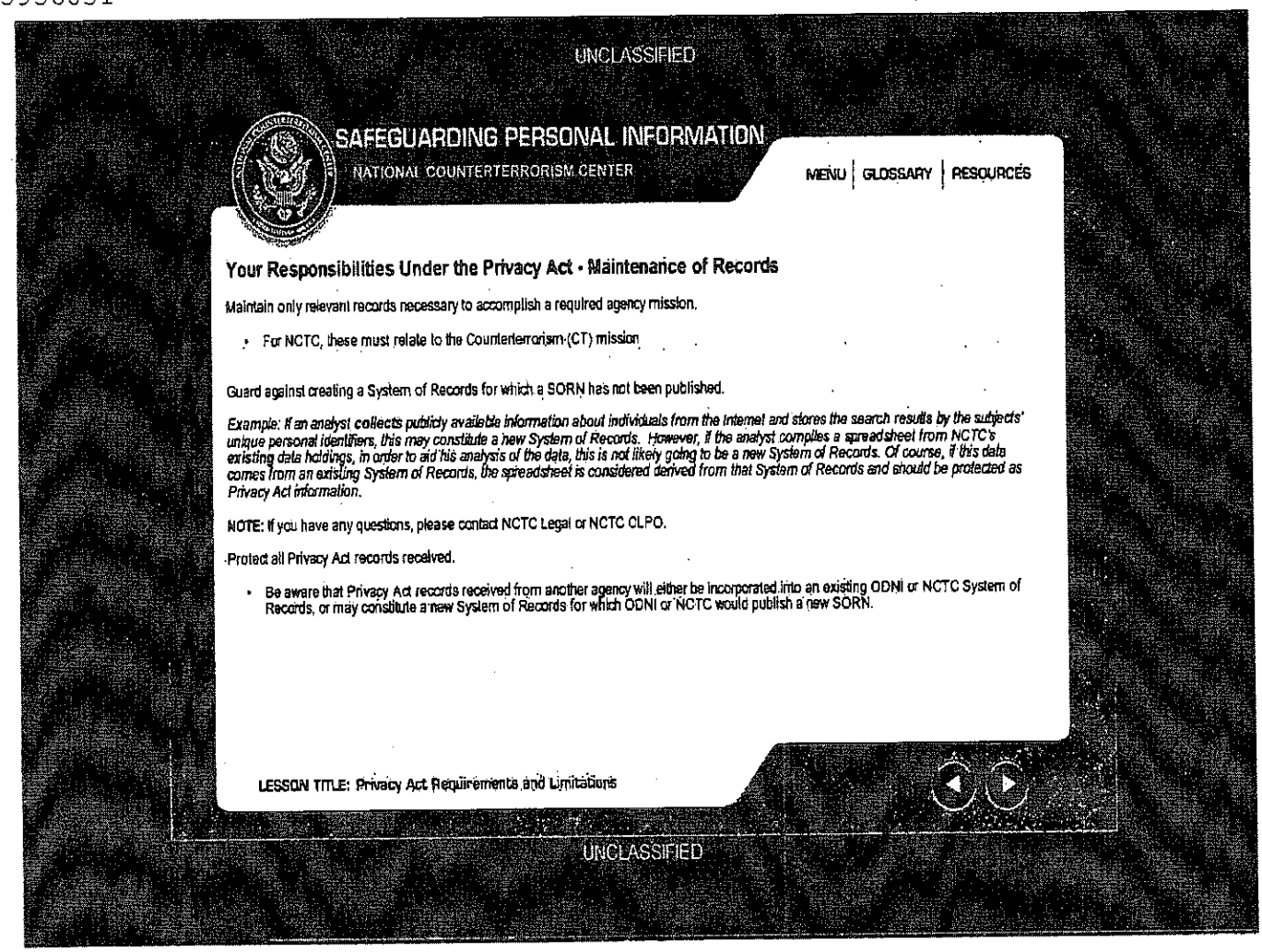
LESSON TITLE: Privacy Act Requirements and Limitations

UNCLASSIFIED

C05956031


UNCLASSIFIED
SAFEGUARDING PERSONAL INFORMATION
NATIONAL COUNTERTERRORISM CENTER
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
UNCLASSIFIED

C05956031


UNCLASSIFIED
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 subjects' 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
UNCLASSIFIED

C05956031

UNCLASSIFIED

SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERTERRORISM CENTER

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

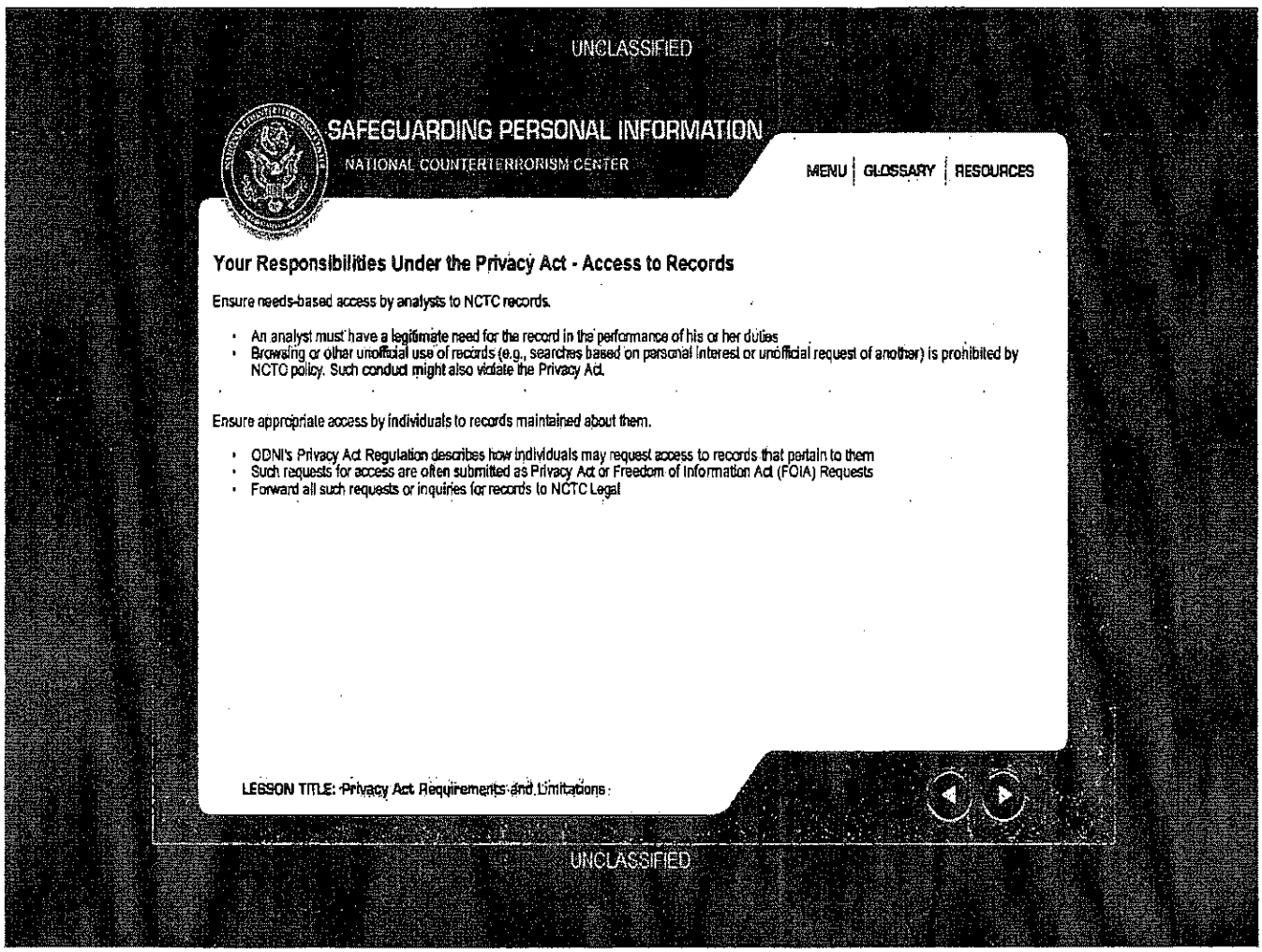
Watch for records describing First Amendment activities!

- 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.

UNCLASSIFIED

C05956031


UNCLASSIFIED
SAFEGUARDING PERSONAL INFORMATION
NATIONAL COUNTERTERRORISM 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
UNCLASSIFIED

C05956031

UNCLASSIFIED

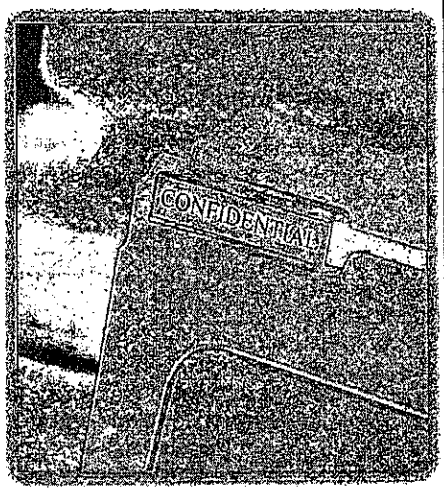
SAFEGUARDING PERSONAL INFORMATION

NATIONAL COUNTERTERRORISM CENTER

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