Annual Privacy Act Training & Safeguarding Personally Identifiable Information

Presented by the DoDEA Privacy Office
(For 2011 – SY 2011/12)

Next

Training Requirements

This training is required under DoD 5400.11-R, DoD Privacy Program; and OSD Administrative Instruction 81.

All DoDEA employees, managers, supervisors, and contractors who have access to PPI/PII are required to complete this training.

When responding to questions, please choose the BEST response.

In order to receive credit for completion of this training, employees must complete the certificate that is provided at the end of the course and submit it through their appropriate supervisor.

Back

Next

Overview of the Privacy Act of 1974

Main Points

- Statutory/Regulatory Authority
- Purpose of the Act
- Information Protected by the Act
- Primary Features of the Act
- Disclosure
- System of Record Notice
- Privacy Act Statement
- Social Security Number Solicitation
- Individual Request for Record
- Safeguarding Privacy Act Information
- Criminal and Civil Penalties
- Your Role and Responsibility
- Contact Information

Overview of the Privacy Act of 1974

Statutory/Regulatory Authority

Statutory Authority

- **The Privacy Act of 1974, as amended (5 U.S.C. 552a), as implemented by OMB Circular No. A-130**
- DoD Regulatory authority:
  - **DoD Directive 5400.11**
  - **DoD Regulation 5400.11-R**
  - **OSD Administrative Instruction No. 81**

Purpose of the Act

- **The Privacy Act of 1974 was enacted to safeguard individual privacy contained in Federal records and to provide individuals access and amendment rights to records concerning them which are maintained by Federal agencies.**
- **By establishing the Privacy Act, Congress intended to put in proper balance individual privacy with the Government's need to maintain information about individuals.**

Back Next

Overview of the Privacy Act of 1974

Information Protected by the Act

- **Examples of records that are subject to the Privacy Act include:**
  - **Leave Balances; types of leave used**
  - **Home address**
  - **Drug tests and an individual's participation in rehabilitation program**
  - **Home telephone number**
  - **Names of employees who hold government-issued travel cards, including card data**
  - **Complete date of birth**
  - **Personal medical information**
  - **Personal/private information (required for security clearance or similar use)**

Back Next

Overview of the Privacy Act of 1974

Information Protected by the Act – (Cont'd)

- This type of data is now known as Personally Identifiable Information (PII).
- A Privacy Act System of Records exists when a Federal agency maintains information about an individual and retrieves that information by the individual's unique personal identifier (usually name or SSN in DoD)

Overview of the Privacy Act of 1974

Primary features of the Act

- Restricts disclosure of personal information from systems of records.
- Requires Federal agencies to comply with the law for collecting, maintaining, using, and disseminating information from personal records.
- Provides individuals with access to records about themselves.
- Allows individuals to request amendments to records which are inaccurate, irrelevant, untimely, and incomplete.
- Addresses the collection, maintenance use and dissemination of Social Security Numbers.
- Provides legal remedies, both civil and criminal, for violations of the Privacy Act.

Overview of the Privacy Act of 1974

Privacy Definitions

- **Individual**– A living person who is a citizen of the U.S. or is an alien that is lawfully admitted for permanent residence.
  - Not included in the coverage are records that agencies might maintain on non-U.S. citizens or aliens that are not admitted for permanent residence.
    Also not included in the coverage are organizations and businesses, including small businesses, even when the company's trade name is the same as that of the owner.
  - For deceased persons, the release of information is protected when the release would invade the privacy of the surviving next of kin.
- **Personally Identifiable Information**– Information about an individual that identifies, relates or is unique to, or describes him or her; e.g., SSN, medical history, biometrics, date of birth, home address/telephone number.
- **Record** - Any item, collection, or grouping of information, whatever the storage media, about an individual that is maintained by a DoD Component.

Information about an individual that relates or is unique to, identifies, describes him or her, (e.g., Social Security Number, medical history, biometrics, date of birth, home address/telephone number) is called?

a. Interesting
b. Routine Use
c. Personally Identifiable Information
d. Record

Back

a. Incorrect! While information about an individual might be *interesting*, this is not the best response.

Back

b. Incorrect! *Routine Use* is the release of information outside the agency for a purpose compatible with the purpose for which the information was collected.

Back

c. Correct! *Personally Identifiable Information* is information about an individual that identifies, relates or is unique to, or describes him or her, e.g., SSN, medical history, biometrics, date of birth, home address/telephone number.

Back

Next

d. Incorrect! *Record* is any item collection or grouping of information, whatever the storage media, about an individual that is maintained by a DoD Component.

Back

Overview of the Privacy Act of 1974

Privacy Definitions (cont'd)

- **Routine Use** - Release of information outside the agency for a purpose compatible with the purpose for which the information was collected. Releases of information between DoD Agencies (i.e., Army to Navy or any other Defense Department Component) are not considered routine uses. However, a release from the Defense Manpower Data Center to the Veterans Administration would be a routine use.

- **System of records** - A group of records under the control of a DoD Component from which personally identifiable information is retrieved by the individual's name or by some other unique personal identifier.

Back Next

Release of information outside the agency for a purpose compatible with the purpose for which the information was collected is called….?

a. Personally Identifiable Information
b. Individual
c. Files
d. Routine Use

Back

a. Incorrect! *Personally Identifiable Information* is information about an individual that identifies, relates or is unique to, or describes him or her, e.g., SSN, medical history, biometrics, date of birth, home address/telephone number.

Back

b. Incorrect! *Individual* is a living person who is a citizen of the U.S. or an alien lawfully admitted for permanent residence.

Back

c. Sorry! Please try again! *Files* is a term used to describe some or all records and non-record materials of an office or department.

Back

d. Correct! *Routine Use* is release of information outside the agency for a purpose compatible with the purpose for which the information was collected.

Back

Next

Overview of the Privacy Act of 1974

Disclosure

- No agency shall disclose any record which is contained in a system of records by any means of communication to any person or another agency without a written request or prior written consent of the individual to whom the record pertains unless the release has been established by a routine use.
- Disclosure includes any means of communication – oral, written, or electronic.
- Disclosure does not occur if the communication is to those who already know.

Overview of the Privacy Act of 1974

System of Record Notice (SORN)

- Advance public notice must be given before Executive Agencies begin to collect personal information for a new system of records. This is done by publishing a notice in the Federal Register to provide an opportunity for interested persons to comment.

Privacy Act Statement

- The Privacy Act requires that when an agency solicits information from an individual for a system of records the individual must be provided:
  - The statute or executive order of the President that authorizes the agency to solicit the information;
  - The principal purposes for which the information is intended to be used;
  - The routine uses which may be made of the information as published in the SORN in the Federal Register; and
  - Whether the disclosure of the information is mandatory or voluntary; and the effects, if any, on the individual for not providing the information.

A System of Records Notice (SORN) is:

a. A notice received in the mail
b. A notice published in the Federal Register
c. A system where notices are kept in a safe location
d. None of the above

Back

a. Sorry! Please try again! *A notice received in the mail* is not called a System of Records Notice (SORN).

Back

b. Correct!!! A SORN is a notice published in the Federal Register. It informs the public about an Executive Branch Agency's collection of personally identifiable information retrieved by name or other unique personal identifier.

Back

Next

c. Sorry! Please try again! A system where notices are kept in a safe location is not called a System of Records Notices (SORN).

Back

d. Sorry! Please try again!

Back

Overview of the Privacy Act of 1974

Social Security Number Solicitation

- Section 7 of Public Law 93-579 provided that it shall be unlawful to deny any benefit, right, or privilege provided by law because the individual refuses to disclose his or her Social Security Number.

- Any time a SSN is asked for, regardless of whether or not it is to be kept in a system of records, a Privacy Act Statement must be given.

- USD (P&R) Memo, March 28, 2008, "DoD Social Security Number (SSN) Reduction Plan" establishes the DoD policy in the use of the SSN and guidance for reducing its unnecessary use.

Overview of the Privacy Act of 1974

Individual Request for Record

- The individual about whom the record pertains is usually entitled to access his or her own record. The Privacy Act SORN for the pertinent records provides the address one may use to request access to his or her records.
- If the individual believes factual information contained in their record is in error, he or she should follow procedures identified in the system notice for requesting correction of the record. If the system manager refuses to make corrections requested by the individual, the individual may continue to pursue correcting his or her record through the appeal process.

Safeguarding Personally Identifiable Information

What is Personally Identifiable Information (PII)

Personally Identifiable Information is any information about an individual maintained by an agency, including, but not limited to the following:

- **Name;**
- **Social security number;**
- **Date and place of birth;**
- **Photo;**
- **Biometric records, etc., including any other personal information which is linked or linkable to an individual;**
- **Education;**
- **Financial transactions;**
- **Medical history;**
- **Criminal or employment history and information which can be used to distinguish or trace an individual's identity.**

Which of the following is not PII?

a. Date & Place of Birth
b. Criminal History & Biometric Records
c. Social Security Number & Financial Transactions
d. DoD phone number

Back

a. Sorry! *Date & Place of birth* are examples of Personally Identifiable Information (PII).

Back

b. Sorry! *Criminal History & Biometric Records* are examples of Personally Identifiable Information (PII).

Back

c. Sorry! *Social Security Numbers & Financial Transactions* are examples of Personally Identifiable Information (PII).

Back

d. Correct! A *DoD phone number* is not an example of PII.

Back

Next

Safeguarding Personally Identifiable Information

Safeguarding PII

- PII must always be treated as “FOR OFFICIAL USE ONLY” and must be marked accordingly. This applies not only to conventional records but also to electronic (including e-mail) transmissions and faxes, which must contain the cautionary marking “FOR OFFICIAL USE ONLY” and/or “FOUO” whichever is appropriate for the recipient before the beginning of text containing Privacy Act information.
- When e-mailing PII, emails must be encrypted.
- PII may not be sent to personal e-mail accounts.
- Records containing PII should be stored in filing cabinets or other containers so as to prevent unauthorized access.

Safeguarding Personally Identifiable Information

Storing PII

- **Duty Hours**
  - Cover with DD Form 2923 (Privacy Act Cover Sheet) or place in an out-of-sight location when those not authorized access enter the work space.
  - Use filtering devices on computer screens to screen the view.
  - Lock computers when leaving – even for brief periods.
- **After Duty Hours**
  - Records should be placed in a locked drawer, cabinet or office.
- **Special Categories of PII**
  - Personnel Files
  - Investigative Files
  - Security Clearance Files
  - Adverse Action Files
  - Medical Records
  - Any collection of PII that may confer or deny benefits to an individual.

Jane needs to work on the staff report over the weekend. What is the worst way for her to get the data home?

a. E-mail to her personal account
b. Use her government issue laptop
c. Use secure remote access and work on the server
d. Take hardcopy home and ensure it doesn't get lost stolen or viewed by others

Back

a. Correct! PII should never be sent to personal, home, or commercial e-mail accounts.

Back

Next

b. Incorrect! *Using a DoD issued laptop is a secure way to work at an alternate location.*

Back

c. Incorrect! Using secure remote access and working on the DoD Server is a secure way to work from home.

Back

d. Incorrect! Taking a hardcopy of the printout home may not be the most secure way to work from home, but it can be done if the employee takes all the appropriate measures to ensure the documents are not lost, stolen, or viewed by others.

Back

Safeguarding Personally Identifiable Information

Storing PII

- **Sharing PII**
  - Follow the “need-to-know” principle. Share only with those specific DoD employees who need the data to perform official, assigned duties.
- **If the Privacy Act System Manager has granted you authority to make disclosures outside DoD:**
  - Share only with those individuals and entities outside DoD that are listed in the “Routine Use” section of the governing Privacy Act SORN.
- **If you have doubts about sharing data, consult with your supervisor, the system manager, or your component Privacy Officer.**

If you have doubts about sharing PII, who should you consult?

a. Your cubicle mate
b. An Attorney
c. A Security Manager
d. Your Supervisor, Privacy Act Officer or Privacy Act Systems Manager

Back

a. Sorry! Please try again! While the person sitting next to you is knowledgeable about many things, this is not the best person from whom to seek Privacy Act advice.

Back

b. Not quite! Please try again!

Back

c. Not quite! Please try again!

Back

d. Correct! You should consult either your supervisor, the Privacy Act Systems Manager, or your component Privacy Act Officer if there are doubts about sharing Personally Identifiable Information.

Back

Next

Safeguarding Personally Identifiable Information

Transporting PII

- **Using E-mail:**
  - Use Common Access Card procedures
  - Announce in the opening line of the text that FOUO information is contained
  - Encrypt the e-mail before sending
  - Do not send PII to a personal, home or commercial e-mail address
- **Handcarrying**
  - Use DD Form 2923, Privacy Act Data Cover Sheet, to shield contents
- Using Ground Mail:
  - Use kraft or white envelopes
  - May be double wrapped if deemed appropriate
  - Mark the envelope to the attention of the authorized recipient
  - Never use “holey joes” or messenger-type envelopes
  - Never indicate on the outer envelope that it contains PII

When transporting or sending PII, what should you not do?

a. Mail--in white envelope
b. Encrypt the e-mail
c. Send the PII to your personal e-mail account
d. Cover with DD Form 2923, Privacy Act Cover Sheet, hand carry, and hand to the recipient

Back

a. Incorrect! You should *mail in white envelope*.

Back

b. Incorrect! You should encrypt the email.

Back

c. Correct! You should never transmit PII to a personal e-mail account.

It is a reportable breach.

Back

Next

d. Incorrect! You should always *cover with DD Form 2923 when you hand carry documents to recipient's office.*

Back

Safeguarding Personally Identifiable Information

Disposing of PII

- Use any means that prevents inadvertent compromise. A disposal method is considered adequate if it renders the information unrecognizable or beyond reconstruction.

- Disposal methods may include:
  - Burning
  - Melting
  - Chemical decomposition
  - Pulping
  - Pulverizing
  - Shredding
  - Mutilation
  - Degaussing
  - Delete/Empty Recycle Bin

Back

Next

Disposal methods may include all BUT….?

a. Burn bag/shredding when available
b. Melting
c. Tear in half and throw in garbage can
d. Degaussing

Back

a. Incorrect! *Burn Bag/shredding when available* is a method of disposing Personally Identifiable Information.

Back

b. Sorry! *Melting* is a way of disposing Personally Identifiable Information.

Back

c. Correct! *Tearing in half and throwing in garbage cans* is not an appropriate way to dispose of Personally Identifiable Information.

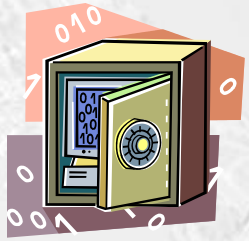
Back

Next

d. Incorrect! *Degaussing* is a method of disposing Personally Identifiable Information.

Back

Safeguarding Requirements



- Three Levels of Safeguards are Required:
  - Administrative
  - Physical
  - Technical

- Individuals are responsible for establishing safeguards:
  - Information Technology System Designers
  - Privacy Act System Managers
  - Local Privacy Act Officials

- Individuals are responsible for seeing that safeguards are applied:
  - YOU!

Who is one person responsible for establishing safeguards?

a. The President of The United States
b. You!
c. Information Technology System Designers
d. Your Supervisor

Back

a. Incorrect! While the *President of The United States* is concerned about the Privacy Act, the President does not establish safeguards.

Back

b. Incorrect! *You* might be responsible for many things, but usually, you are not responsible for establishing safeguards!

Back

c. Correct! *Information Technology System Designers* are responsible for establishing safeguards.

Back

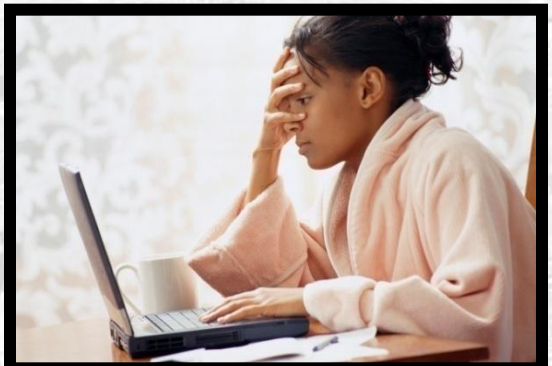
Next

d. Incorrect! *Your supervisor* is responsible for many things, but establishing safeguards for the protection of PII is not one of them.

Back

Information for Teleworkers

- **Paper Records:**
  - Place Privacy Act data in locked drawers, locked briefcases, or other secure areas where family or household members cannot access it.
- **Electronic Records:**
  - Use CAC access and password protection protocols. Share your password and CAC with no one.
  - Save, store and use PII **only** on DoD issued equipment.
  - Do not e-mail PII to your personal, home, or commercial accounts. **This is a breach.**



If You Find Something Questionable

- Immediately notify your supervisor, your component Privacy Officer, the System Manager, or any other appropriate official of the occurrence.

- For World Wide Web postings, make a note of where the information was posted by copying the Uniform Resource Locator (URL). The URL is the address listed at the top of the screen. Most URLs begin http://www.

Wrap Up

Criminal Penalties

- Any agency official or employee who willfully makes a disclosure of a record knowing it to be in violation of the Privacy Act or maintains a system of records without having published the requisite system notice may be convicted of a misdemeanor and fined up to $5,000.

- Any person who knowingly and willfully requests or obtains a record of another individual from an agency under false pretenses may be convicted of a misdemeanor and fined up to $5000.

Wrap Up

Civil Penalties

- The Privacy Act also imposes civil penalties on violators who:
  - Unlawfully refuse to amend a record
  - Unlawfully refuse to grant access to records
  - Fail to maintain accurate, relevant, timely and complete data
  - Fail to comply with any Privacy Act provision or agency rule that results in an adverse effect

- Penalties include:
  - Payment of actual damages
  - Payment of reasonable attorney's fees
  - Removal from employment

Wrap Up

If You Have Access to Personally Identifiable Information

- Protect it at all times.
- Do not share it with anyone unless:
  - The recipient is listed in Section (b) of the Privacy Act or
  - The record subject has given you written permission to disclose it.
- Password protect personal data placed on shared drives, the Internet or the Intranet.
- Monitor your actions: If I do this, will I increase the risk of unauthorized access?
-

Remember:

You may be subject to civil and criminal penalties for violating the Privacy Act.

Wrap Up
Tips for Avoiding Privacy Breaches

- Take privacy protection seriously.
- Respect the privacy of others.
- Alert your supervisor or other management official when you see personal data left unattended.
- Know the Privacy Act requirements.
- Ensure that all message traffic, faxes, and e-mails that contain personal information are properly marked and e-mail is encrypted.
- Do not e-mail PII to a personal, home, or commercial accounts.
- Think Privacy before you seek to establish new data collections on your computer or similar office equipment.

Back Next

Wrap Up

Your Role and Responsibility

Do not collect Personally Identifiable Information without proper authorization.

- Do not maintain illegal files; do not maintain or release inaccurate information.
- Do not distribute or release personal information to individuals who do not have a need for access.
- Do not maintain records longer than permitted.
- Do not destroy records before records retention requirements are met.
- Ensure that you do not place unauthorized documents in a records system.
- Ensure that you mark all documents that contain privacy information “For Official Use Only – Privacy Act of 1974”; or “For Official Use Only – Privacy Act Data.”
- Ensure that all message traffic, faxes, and e-mails that contain personal information are properly marked and e-mail is encrypted.
- Do not e-mail PII to a personal, home, or commercial accounts.
- Think Privacy before you seek to establish new data collections on your computer or similar office equipment.

How to Help Prevent PII

Remove all unnecessary PII information from laptops, memory sticks, portable hard drives, etc., and properly secure all data.

Check all e-mail addresses for accuracy before sending a message containing PII.

When working on PII information at home or on travel ensure all PII is properly secured.

Dispose of PII by using proper disposal methods that renders the information unrecognizable or beyond reconstruction.

Do not place PII on Intranet, Internet or server drive where it can be accessed by unauthorized individuals. Files containing PII must be password protected and available only to those who have a need to know.

Ensure documents containing PII are given to only authorized individuals who have a valid need for the data.

All printed documents with PII data must be covered with a DD 2923 form.

Procedures for a Suspected Breach

If you believe there has been a PII breach, you must report it immediately to:

Ms. Nancy Ramsay (DoDEA Privacy Office)

(703) 588-3202

Nancy.Ramsay@hq.dodea.edu

Also notify your Chain of Command.

Very important to report suspected breach to both immediately!

Procedures for a Suspected Breach

Immediate notification is critical because there are distinct reporting requirements

Provide as much information as possible to the DoDEA Privacy Officer, including a copy of the potentially released material and what persons did/could have access to it. Also include:

- **Who reported the incident and who else has the breach been reported to.**
- **Person who discovered incident - Date & time that the incident was discovered.**
- **Location in which the incident occurred.**
- **Date & time that the incident was reported, if theft involved, date & time reported to law enforcement.**
- **Nature of incident/loss, including a summary of the circumstances and how the breach occurred, what type of PII was involved (name, SSN, birthday, address, salary, health info).**
- **Description of the data and/or information lost or compromised (provide blank forms if applicable).**
- **Storage medium from which data was lost or compromised, e.g., laptop computer, printed paper, etc.**
- **What countermeasures were enabled when the loss or theft occurred, e.g., full computer encryption on laptop file/folder, encryption on certain files on laptop, etc.**
- **If paper documents are lost in transfer, tracking number and name of company shipping package.**
- **Number of individuals potentially affected and a list of their names. POC for follow up and/or actions.**

If a Breach Occurs

The DoDEA Privacy Act Officer must:

- **Notify the DoD Privacy Office of the breach within 48 Hours.**
- **Submit a report to the DoD Privacy Office detailing the specifics of the breach.**
- **Must notify individuals whose PII has been disclosed within 10 days after the loss or compromise is discovered.**

Must advise affected individuals of:

- **What specific data was involved.**
- **The circumstances surrounding the loss, theft, or compromise.**
- **What protective steps the individual can take in response.**
- **What happened, including the date(s) of the breach and of its discovery.**
- **The types of personal information involved in the breach (e.g., full name, SSN, date of birth, home address, account number).**
- **Whether the information was encrypted or protected by other means.**
- **What steps to take to protect themselves from potential harm.**
- **What the agency is doing to investigate the breach, to mitigate losses, and to protect against further breaches.**
- **Who the affected individuals should contact for more information.**

The following PII Breach Scenarios Contain Important Information!

PII Breach Scenarios

- **Is This a Breach?**

Sarah sent Linda, who works for DoD, an unencrypted e-mail with a Social Security Number for Linda to process for payroll. Linda replies to Sarah's e-mail advising her it contained PII and wasn't encrypted.

No! This is not a breach. Although Sarah failed to encrypt the e-mail, Linda did have the "need to know" and the possession and control of the information was never lost. In addition, it was sent via a government system.

Linda should have removed the Social Security Number before replying to Sara to advise her that the e-mail was not encrypted.

Sarah should be reminded by her supervisor to ensure that she encrypts all e-mails containing PII.

PII Breach Scenarios (cont'd)

- **Is This a Breach?**

Sarah is giving a presentation to 10 component employees. She has a slide that has a screen shot of a client's record with name and Social Security Number.

Yes! This is a breach, however, it is a low impact breach.

While Social Security Numbers generally would fall into moderate or high impact risk, the information revealed during the slide presentation had limited adverse effect. The attendees did not have a copy of the slide. There was no loss of possession and control.

This breach would not need to be reported to USCERT.

PII Breach Scenarios (cont'd)

- **Is This a Breach?**

While riding the metro, Sarah lost a roster with a list of an OSD component employees' names, home phone numbers, and addresses, as well as their spouses/children's names.

Yes! this is a medium impact breach. Sarah lost possession and control of the PII. There is the potential for a serious adverse effect on the organizational operational/assets, or individuals if it had been found by someone other than Sarah.

The breach must be reported to USCERT within one hour.

PII Breach Scenarios (cont'd)

- **Is This a Breach?**

Sarah's off tomorrow and it's 4th of July weekend. She needs to get a report done by next week. Her boss will be so pleased if she gets it finished by Tuesday.

Sarah send it to her home yahoo e-mail address so she can work on it over the weekend. It only contains 25 names, Social Security Numbers, DOB and financial information. She lives alone and will be the only one who sees it.

<u>Yes! This is a high impact breach</u>. This breach would have severe or catastrophic adverse effect on the individuals. Sending PII unencrypted is forbidden, especially to a home e-mail address.

This breach must be reported to USCERT within one hour.

Questions or Concerns

Contact

- **DoDEA Privacy Office's website:**
  http://www.dodea.edu/home/dodea.cfm?gnav=pa

- **DoDEA Privacy Office:**
  Nancy Ramsay
  (703) 588-3202
  nancy.ramsay@hq.dodea.edu

Please download and sign the certificate on the next page and provide to your Supervisor.

Certificate of Completion

SY11-12 Privacy Act Training

I certify that I have completed the SY11-12 Annual Privacy Act and Safeguarding Personally Identifiable Information Training and understand my responsibilities in safeguarding and using personally identifiable information.

_____

Type Name

You must sign and submit to your Supervisor

Back

Next

Certification of Completion

FY 2011 Privacy Act Training

I certify that I have completed the FY 2011 Annual Privacy Act and Safeguarding Personally Identifiable Information Training and understand my responsibility in safeguarding and using personally identifiable information.

_____

Type Name

You must sign and submit to your Supervisor

Back Next