Department of the Navy Annual Privacy Training

Screen with blue background and image of thumbprint reader. Clickable "Resources" and clickable "Transcript" link are in bottom right corner.

Click "Start Training" link to begin.

Narrator reads as text appears on screen; images of congressional meetings are shown: In the 1970s, concerns over the quantity of information collected about individuals by the U.S. Government received a lot of public attention. Congress believed it was important to stop unwarranted collection of personal information by the government and to properly protect the personal information that is collected. As a result, the Privacy Act of 1974 was enacted.

Image of female soldier in uniform with her arms crossed.

The Privacy Act has four basic objectives:

- To restrict disclosure of personally identifiable information (PII);
- To grant individuals access to records maintained on themselves;
- To grant individuals the right to correct records that are not accurate, relevant, timely, or complete; and
- To establish a code of "fair information practices" to regulate the collection, maintenance, use, and dissemination of PII on individuals.

Image of male soldier in uniform holding a folder of papers.

In other words, as an individual you have rights. You have the right to know what information is collected about you, how it will be used and by whom, to have it corrected if it is wrong, and to have it protected from unauthorized disclosure to others.

Image of solider in uniform reading paper and holding a pen.

As Department of the Navy military, civilian and contractor personnel you also have responsibilities:

- To only collect and maintain PII about individuals when authorized to do so;
- To only collect the information that is necessary;
- To inform individuals of the authority to collect their information, the principal purpose or use(s) for the collection, to whom it will be disclosed, and the effects on the individual for refusing to provide the information. This is accomplished by providing a Privacy Act Statement, to the individual at the time of collection.

Text on screen: You are also responsible for:

- Ensuring that the information maintained is accurate, relevant, timely and complete;
- Ensuring that PII collected and maintained by the Department of the Navy is kept confidential and is protected against misuse; and
- For knowing what to do if you suspect misuse or if there is a potential or actual compromise of PII.

Image of sailors with retinal eye scanner in background.

The Department of Defense and the Secretary of the Navy have issued guidance to clarify these rights and responsibilities, and to establish privacy programs to ensure that all of the requirements are met. The Department of the Navy Privacy Program affirms that it is the Department's policy that an individual's privacy is a personal and fundamental right that should be respected and protected. Further, Department of the Navy personnel, including contractors, have a responsibility to protect an individual's privacy when collecting, maintaining, using, or disseminating PII about an individual. Failure to properly safeguard PII may result in criminal or civil penalties.

Text scrolls in from the left: POP-UP TIP: The DON CIO is the Senior Component Official for Privacy and oversees the Department's Privacy Program.

Images.

Dramatic changes in information technology have taken place over the past few decades. The digital landscape has evolved and grown well beyond what was considered when the Privacy Act was enacted. Advances in IT capabilities make it possible to generate and maintain significantly greater quantities and increasingly diverse and sensitive types of information. PII may include unique identifiers such as name, date of birth, Social Security Number, DoD ID number, DoD Benefits number, geographic location information and biometrics.

Image of hand typing on a keyboard with text overlaid.

In today's data-driven world, it is necessary for the Navy and Marine Corps to collect, maintain, and use unprecedented volumes of PII. However, there are risks associated with maintaining this information. The evolution of the digital landscape, giving us easier access to a greater volume of information, increases the risk of unauthorized access to, unauthorized disclosure or use of, and loss of PII (also known as a breach). This requires the Department of the Navy to take new and more aggressive approaches to both preventing and responding to breaches of PII.

Image of office building, with text overlaid.

Several Federal agencies have experienced high profile breaches affecting thousands of employees. One of the most notable breaches occurred in June 2015. The Office of Personnel Management (OPM) discovered that the background investigation records of

current, former, and prospective Federal employees and contractors had been stolen. The Office of Personnel Management and the interagency incident response team have concluded with high confidence that sensitive information, including the SSN's of 21.5 million individuals, was stolen from the background investigation databases.

Image of male soldier in uniform holding laptop. Text on screen: What is PII?

To adequately protect PII, you must first understand what PII is. The term PII refers to any information about an individual, including but not limited to, education, financial transactions, medical history, criminal or employment history, and information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number (either full or truncated), date and place of birth, mother's maiden name, address, phone number, biometric information, or any other personal information that can be linked to an individual. This information needs to be protected, because, if compromised, an individual may be put at risk. The compromise of PII can result in embarrassment, inconvenience, reputational harm, financial harm, lower morale, an increased risk to personal security, and identity theft.

Image of man with head in his hands looking depressed.

Identity theft is a significant problem in the United States. Identity thefts represented 16% (490,220) of the over 3 million complaints received by the Federal Trade Commission in 2015 and in 2014, 17.6 million individuals, or 7% of all U.S. residents age 16 or older, were victims of one or more incidents of identity theft.

Perhaps more alarming is that the risk of harm to individuals in today's data-driven economy goes well beyond financial identity theft. Today, malicious actors use stolen PII to create driver licenses, passports, health insurance identification cards, permanent resident cards, and other high-quality identity document forgeries that may then be used to:

- obtain prescription drugs;
- receive medical treatment;
- travel internationally;
- obtain a job;
- claim benefits, such as unemployment;
- file false tax returns to claim a refund;
- obtain authentic government credentials; and
- aid in criminal activities.

Additionally, identity theft can result in embarrassment, inconvenience, financial loss, reputational harm, unfairness, and in rare cases risk to personal safety.

Text scrolls in from the left: POP-UP FACT: If offered credit monitoring and you do not already have it, take it. Be proactive by monitoring your bank accounts and credit report yourself.

Image of female soldier in uniform.

There are many ways that a breach can occur. A breach may occur as a result of human error; intentional, unauthorized disclosure by employees with access to information; or theft by external attackers. Most occurrences result from human error. Knowing what the risks are, and following guidelines and procedures to protect against those risks, is essential to reducing the number of breaches and the harm they may cause.

Image of keyboard with the word "Phishing" and a fishing hook. Text scrolls in from the bottom of the screen.

One of the more common risks that we face is called "phishing." Phishing is a criminal activity in which an adversary attempts to fraudulently acquire sensitive information by impersonating a trustworthy person or organization. Examples of phishing include manipulated emails that appear to be from government agencies, financial institutions, credit card companies, and other recognizable contacts.

The ultimate goal of phishing is to obtain personal information which can then be used to gain access to, or create new accounts.

Training menu screen opens. Three boxes are shown with the titles of "Background," "Email Scenario," and "Work Space Scenario."

The "Background" box contains an image of a laptop computer, as well as the text: In this course, you'll learn basic requirements of the DON Privacy Program, why it's critical to protect PII, and how to handle this sensitive information. A green check mark next to the word "Completed" is underneath this box.

The "Email Scenario" box contains an image of hands typing on a computer, as well as the text: In this training scenario you'll learn how to handle phishing attempts, report breaches, and properly mark and send PII.

The "Work Space Scenario" box contains an image of an office with desks and computers, and the text: In this training scenario you'll learn about common causes of breaches, security controls, and accidental disclosure of PII through a compliance spot check.

At the top of the menu screen is a clickable link with the words "View Your Achievements."

Email Scenario

Mouse over the Email Scenario box and "CLICK TO PLAY" appears. After clicking, a new screen opens with the image of a laptop computer open to an Email Inbox. There are three email messages in the inbox, and the text "Email Scenario; select each email to read it" appears on screen.

Narrator reads: Here is a scenario for you to consider. In this scenario you will be asked to respond to various email messages.

Email One

From: no_reply@online.abcbank.com
Subject: Account Status
Received: 9:15 am

Dear ABC Bank Customer,

Due to recent suspicious online activity, we have temporarily prevented access to your account. ABC Bank safeguards your account when there is a possibility that someone other than you attempts to sign on. You may be getting this message because you signed in from a different location or device. If this is the case, your access may be restored when you return to your normal sign on method.

For immediate access, you are required to follow the instruction below to confirm your account in order to secure your personal account information.

Please respond to this message with:

- *User name*
- *Password*
- *Social Security Number*

Regards, Carter Franke
Chief Customer Service Officer - Card Member Services

Click continue button to proceed to questions.

Narrator reads question: How would you respond to this message?

A. Reply with requested personal information

Text appears on screen: **Incorrect. Please select a different answer.**

This is a phishing attempt. Requests to verify your account, password, or provide PII are red flags which should alert you to these scams. You should never answer any email that attempts to collect PII and other

critical information unless the email has been authenticated. Legitimate financial institutions will never ask for such information via email.

*Click "*Please select a different answer" *to return to question.*

B. Reply with only user name and password

Text appears on screen: **Incorrect. Please select a different answer.**

This is a phishing attempt. Requests to verify your account, password, or provide PII are red flags which should alert you to these scams. You should never answer any email that attempts to collect PII and other critical information unless the email has been authenticated. Legitimate financial institutions will never ask for such information via email.

*Click "*Please select a different answer" *to return to question.*

C. Report the suspicious email to your system administrator or security officer.

Narrator reads and text appears on screen: **Correct.**

This is a phishing attempt. Requests to verify your account, password, or provide PII are red flags which should alert you to these scams. You should never answer any email that attempts to collect PII and other critical information unless the email has been authenticated. Legitimate financial institutions will never ask for this information via email. You could also contact your bank to alert them to the scam.

Click "Continue" to proceed.

D. Ignore the email and delete it from your inbox

Text appears on screen: **Incorrect. Please select a different answer.**

This is a phishing attempt. While you can report this to your command privacy officer, you should always report suspicious email to your system administrator or security officer. Legitimate financial institutions will never ask for this information via email.

*Click "*Please select a different answer" *to return to question.*

After selecting the correct response, a screen opens with the text "Congratulations! You have earned the phishing vanquisher badge." The image of the badge appears on screen.

Click “Continue” to proceed.

New screen opens, and narrator reads text on screen: When you receive a suspicious email, do not respond to or forward it to other users. Do not open attachments, and do not click on any links provided in the email.

Learn to recognize red flags such as:

- unknown sender;
- misspelled words and poor grammar;
- urgent sensational subject lines;
- promises of financial gain, gifts, or prizes;
- requests to verify your password or account.

Email Two

You will return to the screen with the laptop and email inbox. Click on the second email to proceed.

From: cdr.smith32@navy.mil
Subject: Recall Roster

AllPers,

Review your information on the attached recall roster and let me know if it requires updating.

Thanks,

CDR Smith

Click “View attachment” to view recall roster spreadsheet, which includes SSN, name, email, home phone, and home address.

Click “Continue” to proceed to question.

Text appears on screen: You do not have an official need-to-know for the information contained in the attachment. Additionally, the attached document was not marked properly with the required FOUO-Privacy Sensitive disclaimer in accordance with DON policy.

Narrator reads question: Does this represent a PII breach?

A. Yes

Narrator reads and text appears on screen: **Correct.**

CDR Smith sent an unencrypted email containing PII to you and other employees, many of whom did not have a “need to know.” A breach is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar occurrence where (1) a person other than an authorized user accesses or has the ability to access personally identifiable information or (2) a person accesses personally identifiable information for an other than authorized purpose.

Regardless of whether the information was encrypted or not, individuals who do not need to use PII in the performance of their official duties should never have access to someone else’s PII.

Click “Continue” to proceed.

B. No.

Text appears on screen: **Incorrect - please select a different answer.**

A breach did occur due to the disclosure of PII to individuals who did not have a need to know.

A breach is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar occurrence where (1) a person other than an authorized user accesses or has the ability to access personally identifiable information or (2) a person accesses PII for an other than authorized purpose.

*Click “*Please select a different answer” *to return to the question.*

New screen opens with question and answer options.

Narrator reads question: **What action should you take first?**

A. Delete the message.

Text appears on screen: **Incorrect - please select a different answer.**

DON personnel who discover known or suspected losses of PII must report the breaches to their supervisors or privacy officials. You should not delete the message until you have properly reported the breach and been directed to do so.

*Click “*Please select a different answer” *to return to the question.*

B. Reply to CDR Smith.

Text appears on screen: **Incorrect - please select a different answer.**

It's OK to reply to CDR Smith, but remember to not "reply all." DON personnel who have discovered or suspected loss of PII must notify their supervisors or privacy officials.

*Click "*Please select a different answer" *to return to the question.*

C. Upon discovery and within one hour, contact your privacy official or supervisor to report the breach.

Narrator reads and text appears on screen: **Right!**

Within one hour of the discovery of a loss or suspected loss of PII, notify your supervisor or privacy official, who will initiate the PII breach reporting process.

Do not contact the U.S. CERT Office directly. The U.S. CERT Office will be contacted, if necessary, during the PII breach reporting process.

Click "Continue" to proceed.

D. Contact the U.S. Computer Emergency Response Team (CERT)

Text appears on screen: **Incorrect - please select a different answer.**

DON personnel who discover known or suspected losses of PII must report the breaches to their supervisors or privacy officials. You should not delete the message until you have properly reported the breach and been directed
to do so.

*Click "*Please select a different answer" *to return to the question.*

New screen opens with question and answer options.

Narrator reads question: What should CDR Smith have done to prevent this PII breach?

A. CDR Smith should have labeled the email attachment with the privacy warning "FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE: Any misuse or unauthorized disclosure of this information may result in both criminal and civil penalties."

Text appears on screen: **Wrong – Please select a different answer.**

Sending an email containing PII is acceptable if the proper controls are in place.

i. Before sending an email ask the question “Do the recipients have a need to know?”
ii. Official emails containing PII must be digitally signed and encrypted.
iii. All electronic or paper copies of documents containing PII must be marked with the following: “FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE: Any misuse or unauthorized disclosure of this information may result in both criminal and civil penalties.”

Click “Please select a different answer” to return to the question.

B. CDR Smith should not have sent an unencrypted email containing everyone’s PII to individuals who did not have a need to know.

Narrator reads and text appears on screen: **Correct.**

CDR Smith should always send PII in a digitally signed and encrypted email and should never send PII to recipients that do not need to know the information for the performance of their official duties.

Click “Continue” to proceed.

C. CDR Smith should not have sent an unencrypted email containing PII via email.

Text appears on screen: **Wrong – Please select a different answer.**

Sending an email containing PII is acceptable if the proper controls are in place.

i. Before sending an email ask the question “Do the recipients have a need to know?”
ii. Official emails containing PII must be digitally signed and encrypted.
iii. All electronic or paper copies of documents containing PII must be marked with the following: “FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE: Any misuse or unauthorized disclosure of this information may result in both criminal and civil penalties.”

Click “Please select a different answer” to return to the question.

Once the correct answer is chosen, a new screen opens with the text "Congratulations! You have earned the Breach Reporting Badge, with an image of the badge.

Click "Continue" to proceed.

Email Three

You will return to the screen with the laptop and email inbox. Click on the third email to proceed.

From: pat.z.anderson@navy.mil
Subject: Overseas Travel Form

Received: 7:22 am

Good afternoon,

I was informed by your manager that you will be taking an overseas trip soon. For security purposes, please fill out the attached form and return it to me as soon as possible.

Thank you,
Pat Anderson
Department of Human Resources

Click "View attachment" to view form.

Click "Continue" to proceed to question.

Narrator reads question: What action should you take first?

A. Report the email to your supervisor or privacy official.

Text appears on screen: **Incorrect – please select a different answer.**

This is a legitimate request for information from a person with a need-to-know, therefore a response is appropriate. However, it is always a good idea to verify any form you are asked to complete. You should ensure you have the most recent version of any official form before providing your PII. Remember to encrypt and digitally sign all emails containing PII.

Click "Please select a different answer" to return to the question.

B. Consult with your command forms manager/admin office or visit the Naval Forms Online website to verify this is an approved form.

Narrator reads and text appears on screen: **Yes!**

It is always a good idea to verify any form you are asked to complete. You should ensure you have the most recent version of any official form before providing your PII. Visit the Naval Forms Online website for a list of approved Naval forms. Remember to encrypt and digitally sign all emails containing PII.

Click "Continue" to proceed to next question.

C. Complete the form and send it back.

Text appears on screen: ***Incorrect – please select a different answer.***

This is a legitimate request for information from a person with a need-to-know, therefore a response is appropriate. However, it is always a good idea to verify any form you are asked to complete. You should ensure you have the most recent version of any official form before providing your PII. Remember to encrypt and digitally sign all emails containing PII.

Click "Please select a different answer" to return to the question.

D. Delete this email.

Text appears on screen: **Incorrect – please select a different answer.**

This is a legitimate request for information from a person with a need-to-know, therefore a response is appropriate. However, it is always a good idea to verify any form you are asked to complete. You should ensure you have the most recent version of any official form before providing your PII. Remember to encrypt and digitally sign all emails containing PII.

Click "Please select a different answer" to return to the question.

Narrator reads and text appears on screen: After completing the form, you are ready to reply to the HR representative and provide them with the requested information, including your PII.

Please select all proper controls for sending PII:

A. Before sending an email ask the question "Do the recipients have a need to know?"
B. The email message is digitally signed
C. The email message is encrypted

D. The body of the email, including any email attachments containing PII, are marked properly (i.e., "FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE. Any misuse or unauthorized disclosure may result in both civil and criminal penalties.")
E. The email subject line contains "FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE" (a best practice)
F. All of the above.

Correct answer: F. All of the above.

Narrator reads and text appears on screen: **Correct.**

All controls mentioned must be in place before sending PII via email.

Click "Continue" to proceed.

Incorrect answer statement (any other selection):

Text appears on screen: **Incorrect – please select a different answer.**

Click "Please select a different answer" to return to the question.

After correct answer is chosen, new screen opens with the text "Hooray! You have earned the Expert Handler Badge, which an image of the badge.

Click "Continue" to proceed.

Work Space Scenario

Mouse over "Work Space Scenario" box and "Click to Play" appears. After clicking box, the image of a male soldier in uniform holding a laptop is shown. The following text is displayed on screen, with a clickable "Let's get started" button.

Narrator Reads: Good morning. I need your help today to complete a privacy compliance spot check. We will be inspecting the office shared drives as well as the physical office space. Let's get started.

Narrator Reads: Recent PII breach reports highlight the need to conduct searches of shared drives throughout the Department to protect employees' PII and reduce the risk of identity theft. PII is found most often in documents related to awards, employment information, performance evaluations, legal documents, medical records, and financial data.

The scanning software we used detected files that contain PII on an unprotected folder.

Narrator reads and text appears on screen: Scanning software detected files that contain PII on an unprotected folder.

To prevent a future breach of this kind, what controls should be put in place?

A. Files that actually contain PII should be password protected.
B. Access to any folders that contain PII should be restricted to only those with an official need-to-know.
C. Determine which documents need to be retained, and when and how to dispose of those documents when they are no longer required.
D. Any documents containing PII should be deleted immediately.
E. A & B
F. A, B, & C

A clickable "Submit" button appears below list of possible answers.

If incorrect response(s) are selected, the following text appears on screen:

> **Incorrect – Click anywhere or press 'Y' to continue.**

Correct answer: F. A, B, & C

Narrator reads the following text, which also appears on screen:

> **You are right!**
>
> All of the controls you selected must be in place before storing PII on a shared drive. If you ever discover files containing PII, and you are not in a position with an official need-to-know, you should report this to your privacy official immediately.
>
> Ensure shared drive access permissions are established and routinely checked. Shared drives are useful tools to store and share information, but they must be properly managed to ensure personnel understand that indiscriminate posting of PII is not authorized. When there is a need to post PII to a shared drive, access to those files must be strictly controlled and routinely monitored for compliance. Problems often occur when network maintenance causes the removal of access controls.
>
> *A clickable "Continue" link is available below the text.*

After clicking "Continue," a screen appears with the text "Bravo! You have earned the Privacy Protector Badge, and an image of a golden "Privacy Protector" badge. A clickable "Continue" link is available below the text.

After clicking "Continue," the same male in uniform holding a laptop returns to the screen.

Narrator reads as text appears on screen: "Great work with the spot check of our shared drive. Now we need to look around the office to identify where our personnel are mishandling PII."

Text at the top of the screen reads: ***Look around the office and identity areas where PII could be mishandled.*** *The image of an office space is on screen with clickable right and left arrows.*

1. Desk:

A stack of white paper documents is sitting on a desk. Click on paper document.

Narrator reads and text appears on screen: Great work! Mary from Human Resources has left a printed form containing PII in plain view. Leaving a document containing PII in an open area is a breach. When hand-carrying documents containing PII it is a best practice to use a Privacy Cover Sheet (DD Form 2923).

Click "Continue" button to return to office space.

2. Fax Machine:

Click on machine:

Narrator reads and text appears on screen: Sharp eye! You've spotted the fax machine. Faxing is one of the least secure means of transmitting information. It often results in the disclosure of PII to personnel who do not have an official need to know.

The use of fax machines to send information containing Social Security Numbers and other PII to DON personnel is prohibited except under the following circumstances:

- When another more secure means of transmitting PII is not practical.

- When a process outside of DON control requires faxing to activities such as the Defense Finance and Accounting Service (DFAS), Tricare, Defense Manpower Data Center (DMDC), etc.
- In cases where operational necessity requires it.
- When faxing PII related to internal government operations only, i.e., office phone number, rank, job title, etc., also called “Rolodex PII.”

Click “Continue” button to return to office space.

3. Blue Recycling Bin:

Click on bin:

Narrator reads and text appears on screen: Ah-hah! You have discovered a printed document containing PII placed erroneously in a recycling bin.

Whenever disposing of PII, always use a burn bag or an approved shredder. Never use a trash can, recycling bin, or dumpster.

Click “Continue” button to return to office space.

4. Office Co-Worker:

A man in a suite stands near a desk. The following conversation text appears:

“Hi there! Did you hear that Susan from the Cybersecurity Team is being reprimanded by her supervisor for being constantly late to work?

Response: “No, how did you find that out?”

Person: “I work in the front office, and have access to the boss’s email.”

Click on man.

Narrator reads and text appears on screen: This type of breach is referred to as improper disclosure. Both accidental and improper disclosure of PII can result in legal action or other discipline. You should report this conversation to your supervisor or privacy official.

Once all objects have been clicked, the same male in uniform holding a laptop returns to the screen. Narrator reads and text appears on screen: “Great job! Thanks for helping me complete our privacy compliance spot check.

Click “Continue” button to return to office space.

5. Office Bulletin Board:

Bulletin board with white paper is hanging on the wall. Click on bulletin board.

Narrator reads and text appears on screen: Good catch! You have discovered a recall roster containing SSNs posted in an open area. When creating and sharing a roster of any kind (social, recall etc.):

- Wherever the roster is posted or stored, only those with a need to know should have access.
- Is the information appropriately marked "FOUO - Privacy Sensitive"?
- Limit the collection of PII to the minimum number of elements required to get the job done.
- SSNs, full or truncated, should never be included.
- Provide a Privacy Act Statement any time PII is solicited from an individual, whether in writing or electronically. Contact your Privacy Official for more information.

Click "Continue" button.

After clicking "Continue," the same male in uniform holding a laptop returns to the screen.

Text on screen reads: Great job! Thanks for helping me complete our privacy compliance spot check."

Click "Continue" button.

A new page opens. Narrator reads and text appears on screen: Congratulations you have earned the PII Guardian Badge. The image of the badge appears on screen.

Click "Continue" button.

Main screen opens, with completion checkmarks on all 3 training sections.

Another new screen opens, with text: **Congratulations! You have completed the Department of the Navy Annual Privacy Training.**

Additional Privacy Program resources and references are available on the DON CIO Privacy website at ***http://www.doncio.navy.mil/***

Click the X in the right-hand corner to return to the training.